TEORIE. FISA 1

Securizarea sistemului

Securitatea se referă la menţinerea sistemului în stare de funcţionare în regi continuu şi la parametri normali. Securitatea nu se referă doar la protejarea împotriva diferitelor tipuri de atacuri, ci şi la protecţia împotriva căderilor hardware (a harddisk-urilor), a ştergerii accidentale a datelor.

Un server este supus permanent riscurilor unor atacuri de diferite feluri, aceste provenind de la distanţă sau chiar de pe propria maşină. Atacurile pot fi:

• atacuri de refuz al serviciilor (Denial of Service), care degradează sau defecteaza anumite servicii ale programului;

• atacuri în vederea obţinerii de privilegii asupra sistemului;

• atacuri în vederea copierii sau distrugerii de informaţii.

Principalele tipuri de atacuri:

Poate fi stopat prin introducerea în fişierele de configurare a accesului din cadrul MTA a unei directive de refuzare a mesajelor provenind de pe maşina sau de la utilizatorul respectiv. Această soluţie nu rezolva însă problema traficului prin reţea.

2. **Spam (e-mail spamming)**

De obicei, adresa expeditorului este falsă (pentru a nu putea fi descoperit), astfel că acest tip de atac poate fi prevenit configurând serviciul de e-mail pentru a respinge e-mail-urile provenite de pe domenii care nu pot fi rezolvate.

3. **Falsificarea adresei expeditorului (E-mail spoofing)**

Serverul (sau serverele, în unele cazuri) de mail care a transmis mesajul poate fi determinat prin analiza antetului mesajului. Se recomandă contactarea administra torului serverului respectiv şi solicitarea de informaţii privind originea mesajului (acestea pot fi obţinute din fişierele jurnal ale sistemului)'.

4. **Abonarea nesolicitată la liste de discuţii**

Reprezintă înscrierea unei adrese e-mail pe una sau mai multe liste de discuţii fără ca persoana căreia îi aparţine adresa să fi cerut explicit acest lucru. Nu există soluţii rapide pentru stoparea acestor atacuri, ci doar trimiterea de cereri de dezabonare. :

5. **Atacuri pentru refuzul serviciilor (Denial of Service)** '

Prevenirea atacurilor de tip DoS se poate face prin instalarea de firewalluri (care să filtreze pachetele către porturi care trebuie protejate, precum şi pachetele ICMP) instalarea de conexiuni de siguranţă (backup) şi dezactivarea serviciilor care n necesare (pentru a diminua expunerea acestora la potenţialele atacuri).

6. **Depăşirea zonelor tampon**

Acest tip de atac nu poate veni însă din afara maşinii, ci din interiorul și nu poate fi prevenit. Pe măsură ce asemenea erori sunt descoperite, sunt generate actualizări ale programelor.

7. **Interceptarea reţelei (IP sniffing)**

Un asemenea atac se poate preveni doar din interiorul reţelei locale. Pentru a preveni, este bine să utilizăm, cel puţin pentru transmiterea parolelor din protocoale sigure, criptate, cum ar fi SSH.

8. **Cai troieni (Trojan horses)**

Toate fişierele executabile sau arhivele conţinând programe descărcate de pe Internet (chiar şi de pe şiturile oficiale) trebuie verificate înainte de a fi instalate și executate. De asemenea, se recomandă realizarea periodică de copii de siguranță a sistemelor de fişiere, pentru a putea restaura fişierele executabile originale în alterării acestora de către cai troieni.

9**. Uşi ascunse**

Uşile ascunse sunt cazuri particulare de cai troieni. Un asemenea program creează o „poartă" (de exemplu, un utilizator nou) care să permită accesul ulterior la calculatorul în cauză sau să acorde unui anumit utilizator privilegii speciale. Spre

exemplu, un cal troian poate înlocui fişierul /bin/login, care are rolul de a autentifica utilizatorii, pentru a salva parolele tastate de aceştia într-un fişier ascuns;

10. **Viruşi**

Viruşii sunt programe care pot efectua operaţiuni nedorite, de obicei distructive, şi care au capacitatea de a se „multiplica", adică de a infecta şi alte programe. Viruşii rezidă în general în cadrul fişierelor executabile. Sistemele UNIX nu sunt vulnerabile la viruşi, datorită gestiunii stricte a memoriei şi a proceselor care se execută. Este recomandat, în orice caz, să nu se execute ca root nici un fişier executabil despre care nu se cunoaşte ce face.

11. **Viermi (Worms)**

Viermii sunt programe de sine stătătoare, capabile să se multiplice, să se transfere pe alte calculatoare şi, eventual, să efectueze operaţii distructive. Sistemele FreeBSD nu sunt afectate de viermi.

12. **Ghicirea parolelor (password guessing)**

Acest tip de atac se referă la folosirea unui program pentru a determina parolele prost alese, denumit în genere spărgător de parole (cracker). Un astfel de program poate determina, printr-o analiză comparativă, o corespondenţă între variantele de presupuse parole criptate.

13. **Folosirea de anumite vulnerabilităţi (bugs) a programelor / serviciilor existente pe server**

De obicei, problema securităţii nu se pune la nivel de nucleu al sistemului de operare, ci la nivelul aplicaţiilor. La anumite perioade de timp sunt descoperite vulnerabilităţi în aplicaţiile instalate în sistem, în servicii, unele dintre ele putând fi folosite pentru a obţine accesul în sistem.

Reuşita atacurilor este de cele mai multe ori cauzată de configurări slabe ale sistemului sau de neglijarea erorilor (bugs) de securitate descoperite şi de lipsa update-uui la timp a programelor ce prezintă vulnerabilităţi. De aceea trebuie acordată o importanţă mare configurărilor de după instalare.

Acțiuni ce trebuie întreprinse pentru a se asigura securizarea unui sistem de operare în rețea:

- Siguranţa fizică a sistemului - Instalarea maşinii trebuie realizată într-un loc sigur, să nu fie expusă contactului cu persoane neautorizate. Acestea nu trebuie să aibă posibilitatea sau timpul necesar de a înlătura carcasa, de a modifică configuraţia hardware, de a opri şi apo reporni maşina (eventual în modul single), de a înlocui sau copia informaţiile discuri sau de a inocula programe răuvoitoare (cai troieni). De asemenea, mediile de stocare a salvărilor de siguranţă trebuie să fie păstrate într-un loc închis, fără posibilitate de acces (e.g., un seif).
- Salvările de siguranţă - Se recomandă salvarea periodică cel puţin a fişierelor importante şi, dacă este posibil a întregului conţinut al sistemelor de fişiere.
- Drepturile de acces la fişierele importante - Trebuie acordată o atenţie sporită drepturilor de acces la fişierele importante: fişierele de configurare ale diverselor servicii instalate în sistem, fişierele jurnal (log-uri), executabilele care nu trebuie să poată fi apelate de către utilizatorii obişnuiţi, precum şi alte fişiere importante (spre exemplu, baze de date MySQL, PostreSQL etc.), executabilele şi scripturile de iniţializare ale sistemului nu trebuie să poată fi modificate decât de root / administrator.
- Execuţia daemonilor / proceselor - Se recomandă ca numai daemonii / procesele utilizaţi(te) curent să ruleze pe sistem. Mai mulţi(te) daemoni / servicii înseamnă o încărcare mai mare a sistemului, precum şi un nivel de vulnerabilitate mai mare. De asemenea, o mare parte a daemonilor / serviciilor (care oferă diverse servicii) nu trebuie executaţi sub root / administrator, ci sub utilizatorii speciali (de exemplu, daemonul HTTP rulează sub utilizatorul www).
- Scripturile CGI - Scripturile CGI nu trebuie executate ca root. Acestea trebuie plasate într-un singur director, în care nu se va permite accesul utilizatorilor, iar modificările asupra scripturilor trebuie monitorizate.

- Porturile - Anumite servicii pot fi accesate prin reţea, de pe alte maşini. Pentru aceasta, ele aşteaptă conexiuni pe anumite porturi (e.g., serverul HTTP pe portul 80). Aceste porturi pot constitui puncte vulnerabile ale sistemului (datorită vulnerabilităţilor care pot exista în aceste programe), putând fi detectate de la distanţă cu ajutorul scanerelor. Aceste porturi trebuie protejate fie prin configurarea respectivelor servicii să accepte conexiuni doar de pe o anumită interfaţă de reţea, considerată sigură (e.g., reţeaua locală), fie prin configurarea unui firewall care să nu permită accesarea din exterior a porturilor în cauză.
- Accesul utilizatorului root / administrator în sistem - Din principiu, nu se recomandă permiterea accesului cu root / administrator decât de la consolele sistemului. Accesul de la distanţă (cu SSH) va fi făcut cu un utilizator obişnuit, iar apoi va fi folosită comanda su. Sistemul FreeBSD nu permite accesul la distanţă prin SSH folosind autentificarea ca root şi, de asemenea, nu permite su decât din contul utilizatorilor ce aparţin grupului wheel.

ACTIVITATEA 1

1. In fisa de teorie este prezentat pe scurt principalele tipuri de atacuri venite in principal din exteriorul retelei. Creati un referat in care sa prezentati un program cu ajutorul caruia creati un backup al unui server (fisiere si sistem de operare)

Tema 1

Noţiuni de bază în securitate – nivele minime de securitate acceptabile

TEORIE. FISA 1

Ca o definiţie, sistemul de calcul reprezintă un ansamblu de componente hardware (dispozitive) şi componente software (sistem de operare şi programe specializate) ce oferă servicii utilizatorului pentru coordonarea şi controlul executării operaţiilor prin intermediul programelor.

Principiile de bază ale securităţii sistemelor informatice s-au schimbat relativ puţin în ultimii ani. Există două mari categorii – *protecţia la nivel fizic* (garduri, uşi cu încuietori, lacăte, etc.) şi *la nivel informaţional* (accesare prin intermediul unor dispozitive electronice şi/sau a unor aplicaţii software, a informaţiilor dintr-un sistem de clacul).

Securitatea sistemelor informatice

Ca şi concepte distincte care tratează problema securităţii deosebim:

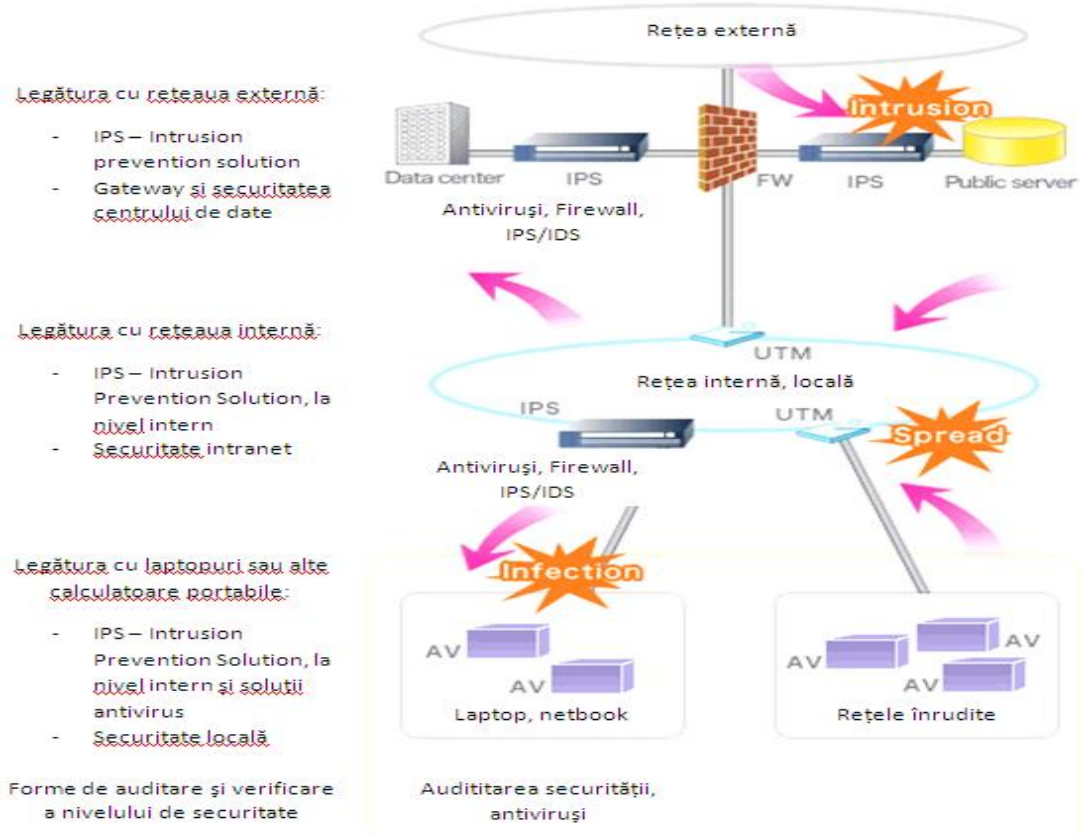
- securitatea bazată pe mai multe nivele – **security in depth**;
- securitatea implementată încă din faza de proiectare – **security by design.**

Pentru a reduce riscurile de securitate în utilizarea şi administrarea sistemelor IT, cea mai bună strategie este cea pe ansamblu (security in depth). Aceasta presupune evaluarea pe ansamblu a infrastructurii IT şi clasificarea expunerii la riscuri de securitate. Pentru fiecare dintre riscurile identificate trebuie realizate planuri de măsuri, fie pentru reducerea expunerii la acele riscuri (**mitigation**), fie pentru reducerea impactului odată ce riscul s-a produs (**contingency**).

La polul opus se află abordarea punctuală (limitată în a oferi protecţie doar la un anumit nivel), a implementării unui sistem specific de securitate, de exemplu antivirus sau detectarea accesului neautorizat (Intrusion Detection Systems – IDS). Deşi aceste sisteme sunt foarte utile în cadrul ariei specifice de aplicabilitate, această abordare lasă descoperite alte zone cu posibile breşe de securitate.

Pentru a avea o abordare de ansamblu, trebuie pornit de la lucrurile elementare: uniformitatea infrastructurii din punct de vedere al sistemelor folosite, administrarea centralizată, menţinerea la zi a sistemelor din punct de vedere al patch-urilor şi fix-urilor (pentru sistemele de operare şi aplicaţiile instalate), aplicarea unor configurări standard de securitate pe toate serverele şi staţiile de lucru, în funcţie de rolul funcţional al acestora precum şi realizarea unor proceduri standard de utilizare şi administrare.

Studiile arată că în medie 90% din breşele de securitate identificate nu sunt datorate problemelor tehnologice ci instalării şi configurării necorespunzătoare sau datorită nerespectării unor proceduri de utilizare şi administrare a sistemului. În multe cazuri, aceste proceduri nici nu există. Trebuie deci să privim problema pe ansamblu, adresând tehnologia, oamenii şi procedurile interne ale companiei/organizaţiei.



Securitatea la nivel de acces perimetral şi la nivel informaţional

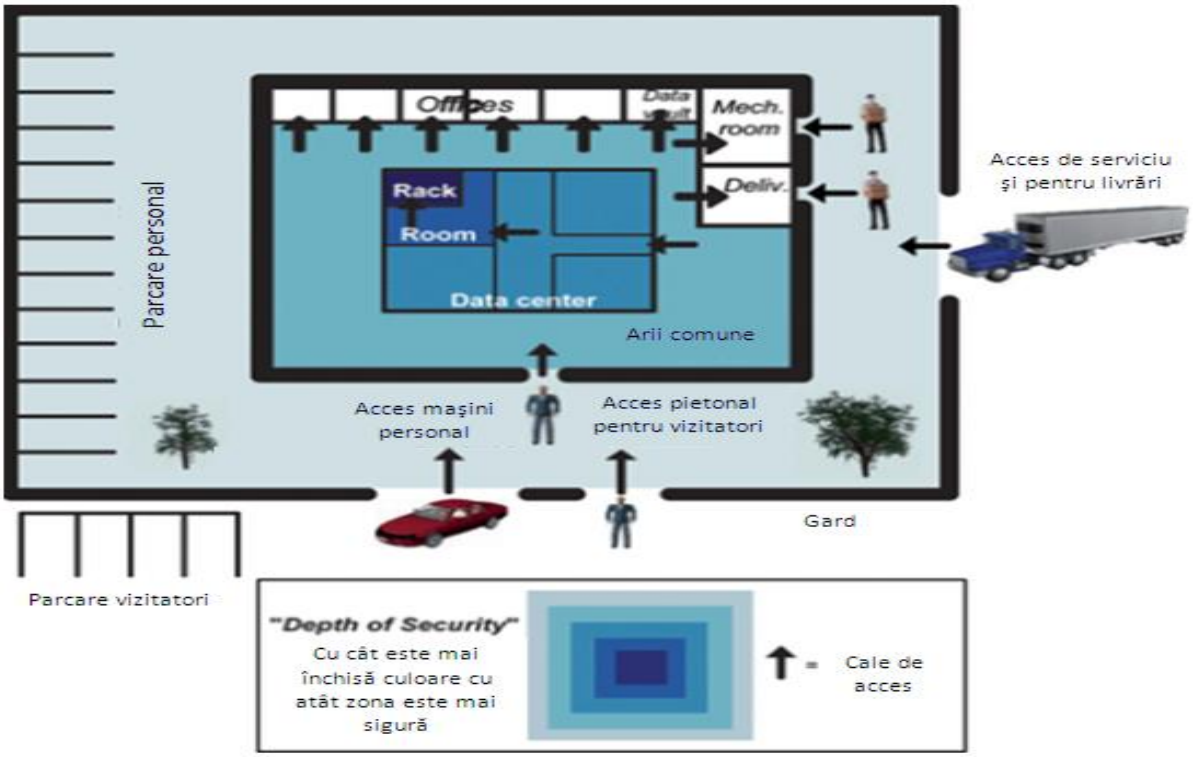
Securitatea trebuie să fie o caracteristică intrinsecă a sistemului. Un sistem sigur este unul bine proiectat, implementat, utilizat şi administrat.

Conceptul de „*security by design*” este foarte bun atunci când posibilităţile de implementare sunt justificate. De multe ori totuşi acest concept impune unele restricţii care limitează foarte mult utilizarea sa în arii diferite, metoda fiind folosită în zone speciale, foarte specializate (zone cu statut de importanţă majoră, ca de ex. reţelele de calculatoare care controlează traficul aerian, laboratoare de cercetare, etc.), zone în care accesul prin definiţie este foarte restrictiv.

Exemplu de folosire al conceptului de „security by design” în viaţa de zi cu zi

Acest concept aplicat la „nivel software” generează un principiu de funcţionare al aplicaţiei cu restricţii foarte clare şi puternice – care de multe ori din pricina acestor limitări devine în scurt timp inutil.

„*In-depth security*” sau „*defence in depth*” este un principiu bazat pe mai multe „straturi” de securitate în vederea protejării sistemului sau reţelei din care face parte.



Evidenţierea conceptului de „Security in depth”

Trebuie să se înţeleagă că nu contează cât de de bun este fiecare „strat” – privit singular, există cineva mai deştept, cu resurse materiale şi temporale suficiente cât să treacă de acesta. Acesta este motivul pentru care practicile uzuale de securitate sugerează existenţa mai multor nivele de securitate sau pe scurt „in-depth security”.

Folosirea de nivele(layers) diferite de protecţie, de la diferiţi producători oferă o protecţie substanţial mai bună.

Folosind o securitate bazată pe diferite nivele de protecţie veţi fi protejaţi de majoritatea persoanelor răuvoitoare, cu excepţia celor mai deştepţi şi mai dedicaţi. Ca o regulă de bază (nivele minime de securitate instalate) se sugerează următoarele produse:

- **firewall** – o barieră protectivă între calculator, reţeaua internă şi lumea din jur. Traficul din interior şi spre exterior este filtrat, restricţionat, blocând eventualele transmisii nenecesare. Folosind reguli stricte de acces la nivel de aplicaţii şi utilizatori, se poate îmbunătăţi substanţial securitatea sistemului şi a reţelei locale;
- **antivirus** – un software instalat cu scopul clar de a te proteja de viruşi, viermi şi alte coduri maliţioase. Majoritatea aplicaţiilor antivirus monitorizează traficul în fiecare moment, scanând în timp ce se navighează pe Internet sau scanând mesajele primite pe mail (cu tot cu ataşamente) şi periodic oferind posibilitatea rulării unei scanări la nivelul întregului sistem în căutarea de cod maliţios;

Atenţie totuşi la aplicaţiile care se dau drept aplicaţii antivirus

Intrusion Detection System (IDS) şi Intrusion Prevention System(IPS o varianta mai specială a IDS) – un dispozitiv sau o aplicaţie folosit(ă) pentru a inspecta întregul trafic dintr-o reţea şi de a trimite mesaje de alertă utilizatorului sau administratorului sistemului cu privire la încercări neautorizate de acces. Principalele metode de monitorizare sunt cele bazate pe semnături şi cele bazate pe anomalii. Funcţie de metodele folosite IDS-ul poate rămâne la stadiul de a alerta utilizatori sau poate fi programat să blocheze automat traficul sau chiar programat să răspundă într-un anumit fel.

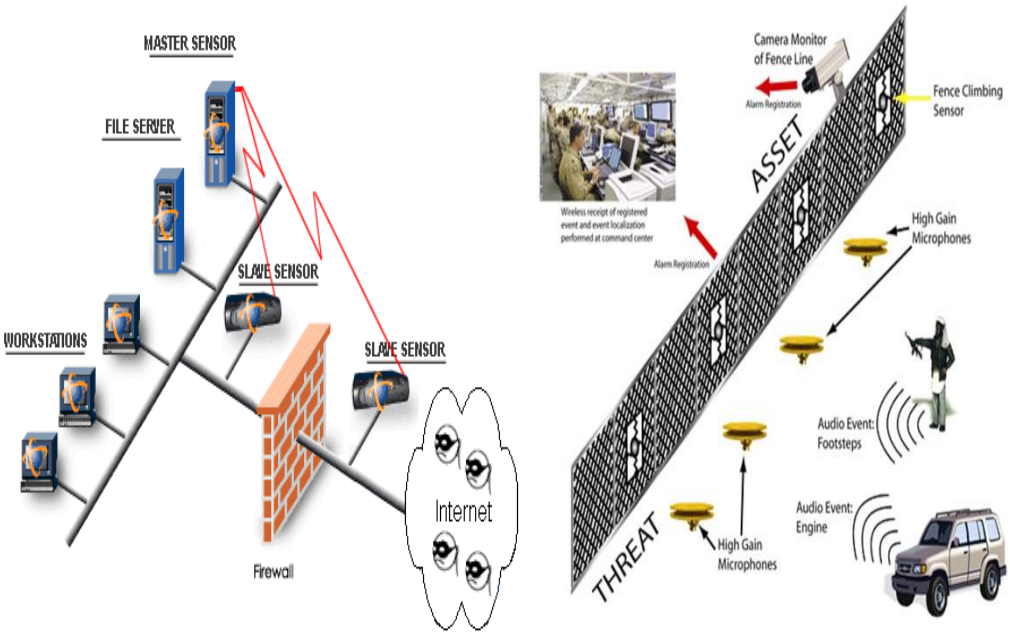
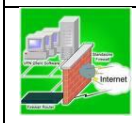
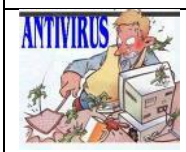


Fig. 1.1.6 IDS la nivel software şi hardware

ACTIVITATEA DE ÎNVĂŢARE NR.1

1. Având la dispoziţie următorul tabel, bifaţi corespunzător categoriei din care face parte fiecare imagine(text).

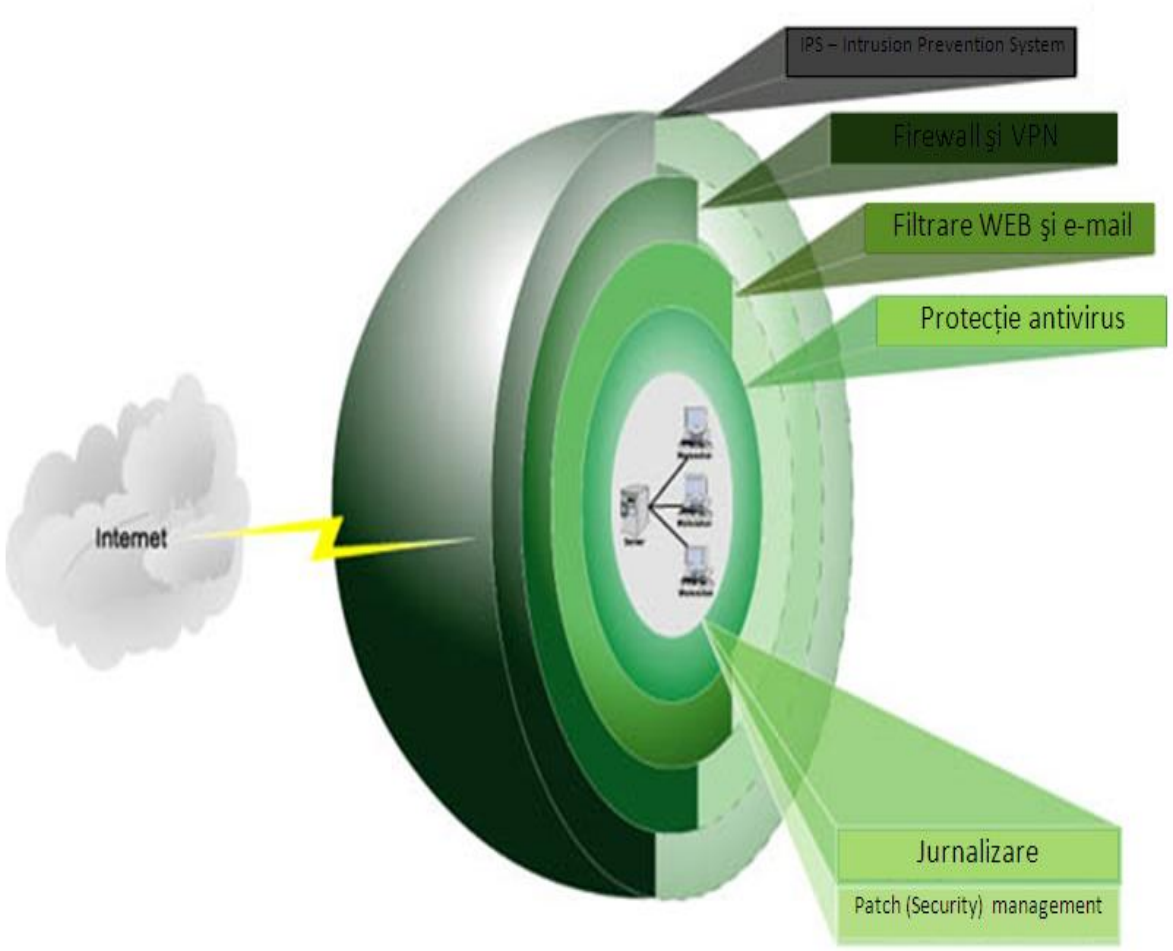
Imagine / text	Categoria din care face parte	
	Securitate la nivel fizic	Securitate la nivel informatic
 Lacăt		
 Uşă metalică		
 Firewall		
 Antivirus		
 Cabinet servere		
 Intrusion Detection System (IDS)		
 Router		

2. Un informatician trebuie să conceapă un model de securitate bazată pe mai multe nivele pentru protecţia unui server. Câte (precizaţi şi motivul) nivele minime de securitate consideraţi că trebuie să acopere acesta?

TEORIE. FISA 2

Noţiuni de securitate a reţelelor de calculatoare

Pentru a se putea înţelege ceea ce doreşte a se „apăra” în cadrul reţelei, se vor prezenta mai întâi natura atacurilor ce pândesc o reţea de calculatoare. Acestea se identifică în trei mari categorii: *confidenţialitate*, *disponibilitate* şi *integritate*. Între acestea există o interdependenţă foarte strânsă, evidenţiindu-se faptul că disponibilitatea şi confidenţialitatea sunt efectiv legate de integritate.



Nivele distincte pentru creşterea securităţii unei reţele

Pentru a înţelege ceea ce se ascund în spatele acestor trei noţiuni, să detaliem:

a) Atacuri care se referă la **integritatea reţelei** ca sumă de echipamente interconectate şi a legăturilor dintre acestea şi/sau la integritatea datelor ce circulă în cadrul ei. Această categorie generează politici diferite prin prisma celor două forme de integritate: fizică – a echipamentelor şi legăturilor dintre acestea şi informaţională – relativ la date şi folosirea lor. Ca definiţii acceptate pentru integritate deosebim: *integritatea datelor* – se referă la

calitatea, autenticitatea, corectitudinea şi acurateţea informaţiilor stocate într-un sistem informatic şi *integritatea sistemelor* – drept posibilitatea operării corecte şi cu succes a resurselor informatice.

b) Atacuri care atentează la **confidenţialitatea sistemului**. Prin aceasta înţelegem informaţia care este disponibilă doar în cazurile în care politicile de securitate sunt îndeplinite. De multe ori această proprietate este atât de importantă încât este cerută de lege sau prin contract.

c) Atacuri care atentează la **disponibilitate** se referă la acele forme de atac care încearcă sau chiar reuşesc să facă inutilizabil sistemul prin privarea posibilităţii de a-şi oferi disponibilitatea (răspunsul şi tratarea cererilor existente) utilizatorilor înregistraţi sau pur şi simplu prin punerea sistemului în forma de „negare a serviciilor".

Reţelele şi resursele ataşate de acestea sunt expuse diferitor tipuri de atacuri potenţiale, cum ar fi: atacuri la integritate (atacuri la autentificare, furtul sesiunilor, atacuri de protocol, tehnici de manipulare – „social engineering", tehnici de manipulare neglijente, abuz de privilegii explorarea uşilor din spate – „backdoors"), atacuri la confidenţialitate (divulgarea neglijentă, interceptarea informaţiei, acumularea informaţiilor) şi atacuri la disponibilitate (interferenţe, supresii, furnizarea de informaţii neaşteptate) forme de atac detaliate în cele ce urmează.

Atacurile de autentificare – situaţia în care o persoană sau un program reuşeşte să se identifice ca o altă persoană/aplicaţie şi astfel să obţină diferite avantaje nelegitime (spoofing). Include furtul direct de parole (shoulder-surfing) sau prin ghicirea sau dezvăluirea acestora. Această formă de atac se poate contracara de cele mai multe ori prin educarea utilizatorilor.

Furtul sesiunilor – o formă prin care un utilizator care a fost autentificat este „înlocuit" de atacator folosindu-se de toate privilegiile acestuia pentru accesul la informaţii sensibile. În cazul prevenţiei, este obligatorie crearea de politici privind aplicaţiile pe care utilizatorii le folosesc sau modul în care sunt folosite precum şi prin utilizarea de aplicaţii antivirus.

Atacurile protocoalelor – de multe ori această formă de atac se bazează pe slăbiciunile sistemelor criptografice. Este o formă „elevată", de multe ori problemele bazându-se pe posibilitatea aflării unor erori matematice sau a unor „slabiciuni" care permit ca o cheie criptografică să fie derivată algebric(sau geometric prin extrapolare). Datorită formei atât de complexe şi elevate, această formă de atac nu poate fi evitată decât printr-o analiză a protocoalelor criptografice de către experţi în domeniu.

Tehnici de manipulare – este o formă de atac care ia amploare prin prisma „încrederii" şi oferirii unor informaţii private, sensibile unor persoane neautorizate. Ca formă preventivă se indică instruirea utilizatorilor suplimentată de o minimalizare a privilegiilor utilizatorilor pentru a reduce efectele unei tehnici de manipulare reuşite.

Metode de acces neglijente – discutăm aici în special de aplicaţia de tip firewall. Mulţi utilizatori din cauza neinformării sau necunoaşterii modului de folosire sau doar din dorinţa de a nu fi „sâcâit" dezactivează această aplicaţie. O formă binecunoscută de prevenţie este segmentarea resurselor între care nu există relaţii pentru a preveni atacuri din alte zone ale reţelei.

O formă specială de atac este cea a **abuzului de privilegii.** Este specială şi din cauza faptului că se referă, la atacurile venite din interior (peste 80%), marea majoritate venind din partea unor angajaţi sau fost angajaţi nemulţumiţi sau în căutarea unor informaţii ce le pot aduce beneficii personale(de ordin material sau nu). Atacurile prin abuzul de privilegii poate fi relativ uşor de contracarat folosindu-se de minimizarea privilegiilor oferite fiecărui utilizator, precum şi prin distribuirea responsabilităţilor mari printre mai mulţi angajaţi.

Folosirea de Backdoors – este o metodă ce se referă la unele „erori" de cele mai multe ori introduse intenţionate în cadrul aplicaţiilor, „erori" ce pot oferi acces la sistemul pe care rulează. O formă gravă a acestei metode este faptul că este foarte greu de depistat şi remediat.

După cum s-a observat exista în formele de atac asupra integrităţii datelor o foarte mare diversitate de metode, aceasta şi din cauza importanţei acesteia (odată „îngenunchiată" aceasta, accesul la celelalte două – confidenţialitatea şi disponibilitatea – este mult mai simplu) în securitatea unei reţele de calculatoare.

Divulgarea neglijentă are lor în momentul în care informaţia devine accesibilă în mod accidental atacatorului. Ca metodă de protecţie se desprinde iarăşi educarea utilizatorilor şi folosirea unor politici de confidenţialitate în concordanţă.

Intercepţia informaţiei – este metoda prin care informaţia este interceptată la momentul trecerii printr-un mediu nesigur, nesupravegheat corespunzător. Ca metodă profilactică se desprinde folosirea de protocoale de criptare precum şi folosirea reţelelor private virtuale (VPN) pentru transferul informaţiilor dintr-o locaţie într-alta.

Metoda acumulării de informaţii se foloseşte de culegerea de informaţii din diferite surse pentru a deduce unele informaţii private. Întrucât este o metodă destul de complexă, protecţia împotriva ei nu este bine definită, fiind legată de totalitatea politicilor de securitate definite şi folosite.

Interferenţele* sau *bruiajele reprezintă una dintre cele mai răspândite forme de atac la disponibilitatea sistemului. O formă foarte răspândită este cea a atacurilor prin inundare, care face ca numărul de procese deschise să fie mai mare decât un sistem a fost proiectat să le efectueze efectiv (ping flood). Succesul unor astfel de forme de atac poate fi limitat sau chiar îndepărtat dacă se introduc unele filtre de admisie şi detecţie sau prin adăugarea de capacitate adiţională.

Supresia jurnalizării este un tip special de interferenţă şi este folosit adesea împreună cu alte tipuri de atacuri. Se folosesc metode prin care efectiv se limitează mesajele jurnalizabile sau prin generarea unui trafic atât de mare încât aflarea propriu-zisă a informaţiei utile să fie foarte dificilă. Metodele de prevenţie se bazează pe analiza statistică a jurnalelor şi implementarea de canale de administrare private.

Furnizarea de informaţii neaşteptate se referă la generarea unui anumit comportament care forţează sistemul să intre în incapacitatea de a-şi continua lucrul. Ca forme de prevenţie se recomandă utilizarea de update-uri şi fix-uri care să trateze corespunzător situaţiile particulare ce pot genera blocarea sistemului respectiv.

Întrucât nu există o autoritate centralizată care să asigure managementul reţelelor este necesar instalarea de diferite nivele de securitate pentru siguranţa

traficului. Dintre aceste nivele menţionăm: firewalls, routers, Intrusion Detection Systems şi alte componente: VPN, criptari etc.

Obiectivele principale ale securităţii reţelelor de calculatoare sunt de a proteja reţeaua, echipamentele şi mesajele din cadrul ei contra accesului neautorizat şi în general de accesul din afara ei. Se pot diferenţia un număr de 3 mari obiective:

1. Să ofere controlul în toate punctele din cadrul perimetrului reţelei pentru a bloca traficul care este maliţios, neautorizat sau prezintă riscuri pentru siguranţa reţelei.
2. Să detecteze şi să răspundă la încercările de pătrundere în reţea.
3. Să prevină mesajele din cadrul ei să fie interceptate sau modificate.

Este de precizat că setările de securitate nu pot elimina complet riscurile. Scopul este de a minimiza efectele pe cât posibil şi să elimine riscurile excesive sau nenecesare (mitigation şi contingency).

Trebuie avut de-asemenea în vedere şi faptul că scopul securităţii reţelei este să ofere conectivitatea la un preţ şi o rată risc/cost acceptabilă.

Principiile securităţii reţelelor de calculatoare se pot sintetiza şi astfel:

a) „Least privilege" – să se dea acces doar dacă este necesar şi doar pentru ceea ce este obligatoriu;

b) Folosirea de nivele de securitate distincte, care să se întrepătrundă (defense in depth) – vezi fişa 1.1

c) Controlul perimetral – plasarea de controale stricte la fiecare capăt de reţea;

d) Refuzarea oricăror drepturi care nu sunt specificate prin exemplificare.

În acelaşi timp totuşi principiile enumerate mai sus trebuiesc să se întrepătrundă cu următoarele:

a) „keep it simple" – trebuie să înţelegi pentru a putea să protejezi;

b) Să ascunzi pe cât posibil informaţiile cu privire la reţea;

c) Tehnologizarea nu este suficientă – o securizare bună constă în mult mai multe decât cele mai recente tehnologii sau „state-of-the-art" software şi hardware;

d) Politici de securitate – absolut necesare pentru a defini nivele de risc şi direcţii generale pentru generarea de practici şi proceduri de securitate şi implementare.

Nu în ultimul rând trebuie menţionat şi rolul utilizatorului final în cadrul întregului concept de securitate, astfel este necesar ca fiecare administrator sau utilizator să încerce să urmeze următoarele sfaturi:

a) jurnalizarea şi monitorizarea – absolut necesară pentru detectarea din timp şi răspunsul prompt la problemele principale;

b) criptarea informaţiilor cruciale care sunt transmise folosind reţele nesigure – informaţiile senzitive care sunt trimise în text simplu pot fi foarte uşor interceptate;

c) nu realizaţi relaţii de încredere bazate pe adrese IP – adresele IP pot fi „spoofed" – „clonate" cu ajutorul unor unelte şi aplicaţii;

d) „weakest link" – un sistem este atât de sigur pe cât este cea mai slabă componentă;

e) Minimizaţi riscul nenecesar – întrucât nu se poate elimina riscul complet, asiguraţi-vă contra riscurilor excesive sau nenecesare (prin realizarea de back-up-uri)

ACTIVITATEA DE ÎNVĂŢARE NR.2

1. Completaţi următorul tabel cu datele de mai jos

Atacuri contra		
confidenţialităţii	**disponibilităţii**	**integrităţii**

cu literele din dreptul textelor din lista de mai jos, asa cum se potrivesc in cele 3 coloane

a) supresii,
b) atacuri la autentificare,
c) furtul sesiunilor,
d) tehnici de manipulare neglijente,
e) furnizarea de informaţii neaşteptate
f) abuz de privilegii,
g) explorarea uşilor din spate – „backdoors”
h) divulgarea neglijentă,
i) tehnici de manipulare – „social engineering”,
j) interceptarea informaţiei,
k) atacuri de protocol,
l) acumularea informaţiilor
m) interferenţe,

2. Realizaţi un eseu care să trateze necesitatea protejării unei reţele, pe baza următoarelor idei: protejarea echipamentelor, protejarea datelor din cadrul reţelei, riscuri acceptabile, conectivitate la un preţ şi o rată risc/cost acceptabilă. Timpul de lucru este de 50 minute iar dimensiunea eseului trebuie să fie de minim o pagină.

Pentru rezolvarea sarcinii de lucru consultaţi Fişa 2 precum şi sursele de pe Internet.

TEORIE. FISA 3

Nivele minime de securitate

Majoritatea companiilor care se ocupă de securitatea sistemelor informatice sunt de acord cu privire la următoarele nivele minime care trebuiesc satisfăcute pentru a fi protejaţi la un nivel minim acceptabil:

a) necesitatea instalării unei aplicaţii de tip anti-virus: aceasta aplicaţie este vitală să fie instalată şi mai mult, să aibă toate actualizările la zi în ceea ce priveşte definiţiile de viruşi;

b) aplicaţie de tip firewall – această aplicaţie a devenit o cel puţin la fel de importantă componentă ca cea anterioară;

c) aplicaţie de tip anti-spyware care să fie la fel, actualizată cât mai des;

d) criptarea informaţiilor cu statut personal, privat;

e)este foarte important şi ca utilizatorul să folosească parole cât mai „bune” şi aici ne referim la lungimea lor (la ora actuală o parolă de 4 caractere se poate sparge într-un timp foarte scurt de ordinul zecilor de minute, la o parola de 8 caractere acest lucru ajungând la ordinul zilelor, mai ales dacă conţin simboluri, cifre şi litere atât mici cât şi mari);

f) nu în ultimul rând este foarte important ca utilizatorul să aibă o conduită precaută, să nu descarce orice programe găsite pe net, să citească orice mesaj de atenţionare venit din partea aplicaţiilor de tip antivirus, firewall, anti-spyware;

g)realizarea periodică de backup-uri ale datelor pentru a putea fi protejat în cazul unor atacuri reuşite sau incidente de genul incendiilor, inundaţiilor sau altor forme asemănătoare.

În definirea unor nivele minime de securitate trebuiesc obligatoriu luate în considerare, cum am spun şi mai sus costurile. În diagrama de mai jos se poate observa foarte clar ceea ce implică o „complicare” a unei strategii de securitate – evident costuri foarte ridicate(atât în implementare, cât şi în utilizare).

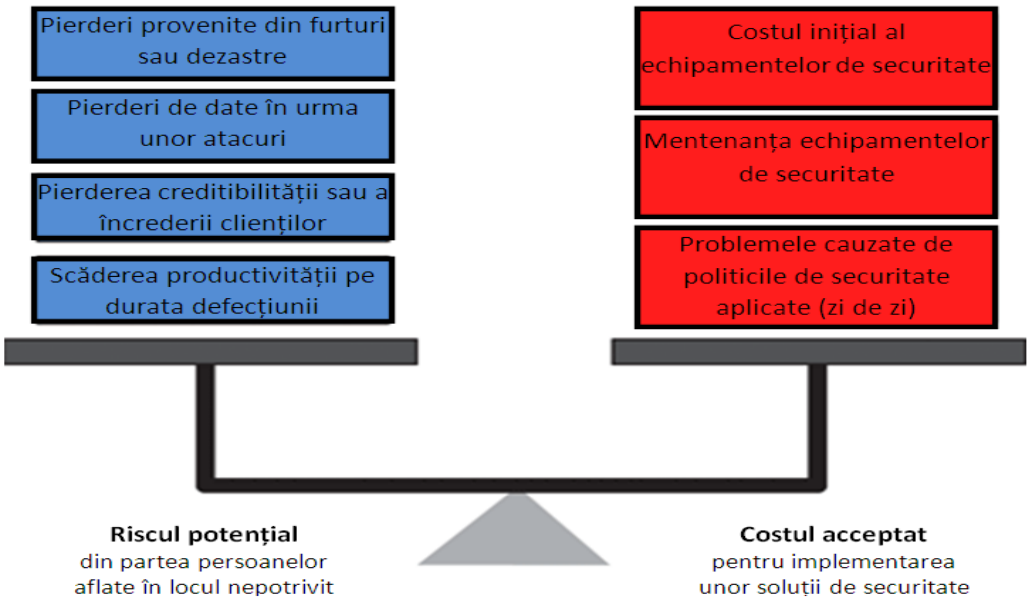


Diagrama decizională în vederea implementării unor nivele minime de securitate

Concluzionând – soluţia corectă cu privire la toleranţa riscului versus costul implementării şi utilizării – trebuie să ţină cont de următoarele:

a). Costul potenţial în cazul unei breşe de securitate – aici se detaliază cazurile: *pierderi fizice* – accidente prin care rezultă pierderea încăperilor(cutremur, foc, apă, explozii, etc.) şi/sau echipamentelor(sabotare, furt, etc.), *pierderi la nivel de productivitate* – diversiunea persoanelor de la posturile lor pentru repararea sau înlocuirea unor echipamente, reconstrucţia datelor sau până echipamentele per ansamblu sunt inaccesibile, *pierderea la nivel de organizaţie* – întreruperea întregii afaceri până la remedierea problemelor apărute, *pierderea de informaţii* – coruperea, furtul sau pierderea efectivă a datelor de pe o anumită perioadă şi, nu în ultimul rând, *pierderea reputaţiei* şi a modului în care este percepută acesta de ceilalţi clienţi – drept o consecinţă a unei breşe de securitate foarte serioase sau a unor accidente repetate care pot conduce chiar la pierderea afacerii, scăderea reputaţiei în rândul clienţilor sau cazul în care informaţiile pierdute pot conduce la acţiuni legale(procese deschise pentru despăgubiri);

b). Costul echipamentelor – limitările impuse de încadrarea într-un anumit buget generează limitarea utilizării excesive a echipamentelor de identificare de ultimă generaţie. Este recomandată folosirea totuşi a echipamentelor de ultimă generaţie măcar la punctele cheie, care găzduiesc informaţiile cheie – gen sala serverelor;

c). Combinarea diferitelor tipuri de tehnologii – combinarea unor tehnologii „low-cost" cu altele mai specializate pe diferite nivele de acces, sau zone sensibile, pot oferi un surplus de securitate la un preţ competitiv;

d). Factorul uman – este foarte important ca factorul uman să fie luat foarte în serios la momentul implementării unor strategii de securitate, întrucât restricţiile pot genera frustrări şi scăderea productivităţii;

e). Scalabilitatea – implementarea incrementală este un procedeu des folosit, implementarea din mers oferind informaţii clare despre necesităţile reale – descoperite în urma folosirii.

Nivelele minime acceptate pot diferi foarte mult de la o implementare la alta, oricare ar fi acestea totuşi trebuie realizată o balanţă între riscurile acceptate şi implementarea unor reguli de securitate foarte complexe sau, din contră, absurde sau inutile.

Software-ul de tip antimalaware(antivirus, anti-spyware).

Scurt istoric: Majoritatea sunt de părere că primul software de tip antivirus este atribuit lui Bernt Fix în 1987, aceasta fiind prima neutralizare a unui virus informatic(nume de cod Viena), cel puţin prima documentată şi publicată. Începând cu anul 1988 încep să apară primele companii care să producă software dedicat (Dr. Solomon's Anti-Virus ToolKit, AIDSTEST, AntiVir) urmat în 1990 de aproximativ 19 programe antivirus distincte, printre care apar şi Norton AntiVirus (achiziţionat de Symantec în 1992) şi McAfee VirusScan.

Ca metode de identificare a viruşilor deosebim:

a) identificarea bazată pe semnătură (signature based) este cea mai comună variantă. Pentru identificarea viruşilor cunoscuţi fiecare fişier este scanat ca şi

conţinut (întreg şi pe bucăţi) în căutarea informaţiilor păstrate într-un aşa-numit dicţionar de semnături;

b) identificarea bazată pe comportament (malicious activity), în acest caz aplicaţia antivirus monitorizează întregul sistem pentru depistarea de programe suspecte în comportament. Dacă este detectată o comportare suspectă, programul respectiv este investigat suplimentar, folosindu-se de alte metode (semnături, heuristic, analiză de fişier, etc.). Este de menţionat că aceasta metodă poate detecta viruşi noi;

c) metoda heuristică (heurisitc-based) este folosită pentru detectarea viruşilor noi şi poate fi efectuată folosind două variante(independent sau cumulat): analiza de fişier şi emulare de fişier. Astfel analiză bazată pe analiza fişierului implică căutarea în cadrul acelui fişier de instrucţiuni „uzuale" folosite de viruşi. Cea de-a doua metodă este cea de emulare în care se rulează fişierul respectiv într-un mediu virtual şi jurnalizarea acţiunilor pe care le face.

d) un mod relativ nou se bazează pe conceptul de semnături generice – ceea ce s-ar traduce în posibilitatea de a neutraliza un virus folosindu-se de o semnătură comună. Majoritatea viruşilor din ziua de astăzi sunt aşa-numiţii – viruşi de mutaţie – ceea ce înseamnă că în decursul răspândirii sale el îşi schimbă acea semnătură de mai multe ori. Aceste semnături generice conţin informaţiile obţinute de la un virus şi în unele locuri se introduc aşa-numitele wildcard-uri – caractere speciale care pot lipsi sau pot fi distincte – aplicaţia software căutând în acest caz informaţii non-continue.

Observaţii: Este de reţinut că navigând la întâmplare se pot găsi o multitudine de aplicaţii care să „pozeze" în aplicaţii de tip antivirus, antispyware sau antimalaware – dar de fapt să fie ele însele viruşi deghizaţi în aplicaţii legitime.

Aplicaţiile de tip Firewall

O aplicaţie de tip firewall, lucrează îndeaproape cu un program de rutare, examinează fiecare pachet de date din reţea (fie cea locală sau cea exterioară) ce va trece prin serverul gateway pentru a determina dacă va fi trimis mai departe spre destinaţie. Un firewall include de asemenea, sau lucrează împreună, cu un server proxy care face cereri de pachete în numele staţiilor de lucru ale utilizatorilor. În cele mai întâlnite cazuri aceste programe de protecţie sunt instalate pe calculatoare ce îndeplinesc numai această funcţie şi sunt instalate în faţa routerelor.

Soluţiile firewall se împart în două mari categorii: prima este reprezentată de soluţiile profesionale hardware sau software dedicate protecţiei întregului trafic dintre reţeaua unei întreprinderi (folosită la nivel de instituţii ex. universităţi, sit-uri Web, etc.) şi Internet; iar cea de a doua categorie este reprezentată de firewall-urile personale dedicate monitorizării traficului pe calculatorul personal. Utilizând o aplicaţie din ce-a de a doua categorie veţi putea preîntâmpina atacurile utilizatorilor care încearcă să acceseze sistemul.

Concluzionând, putem spune că un firewall este folosit pentru două scopuri majore: pentru a păstra în afara reţelei utilizatorii rău intenţionaţi şi pentru a păstra utilizatorii locali (angajaţii, clienţii) în deplină securitate în reţea.

Înainte de a construi un firewall trebuie hotărâtă politica sa, pentru a şti care va fi funcţia sa şi în ce fel se va implementa această funcţie.

Politica firewall-ului se poate alege urmând câţiva paşi simpli:

- se alege ce servicii va deservi firewall-ul;

- se desemnează grupuri de utilizatori care vor fi protejaţi;
- se defineşte ce fel de protecţie are nevoie fiecare grup de utilizatori;
- pentru serviciul fiecărui grup se descrie modul cum acesta va fi protejat;
- se defineşte o regulă generică prin care oricare altă formă de acces este respinsă.

Politica este foarte posibil să devină tot mai complicată odată cu trecerea timpului, de aceea este bine să se documenteze toate modificările făcute de-a lungul utilizării ei.

Pentru a înţelege mai bine menirea unui firewall să precizăm ce poate şi ce nu poate să facă.

O aplicaţie firewall poate:

a) să monitorizeze căile de pătrundere în reţeaua privată, permiţând în felul acesta o mai bună monitorizare a traficului şi deci o mai uşoară detectare a încercărilor de infiltrare;

b) să blocheze la un moment dat traficul în şi dinspre Internet;

c) să selecteze accesul în spaţiul privat pe baza informaţiilor conţinute în pachete;

d) să permită sau să interzică accesul la reţeaua publică, de pe anumite staţii specificate;

e) şi nu în cele din urmă, poate izola spaţiul privat de cel public şi realiza interfaţa între cele două

De asemeni, o aplicaţie firewall nu poate:

a) să interzică importul/exportul de informaţii dăunătoare vehiculate ca urmare a acţiunii răutăcioase a unor utilizatori aparţinând spaţiului privat (ex: căsuţa poştală şi ataşamentele);

b) să interzică scurgerea de informaţii de pe alte căi care ocolesc firewall-ul (acces prin dial-up ce nu trece prin router);

c) să apere reţeaua privată de utilizatorii ce folosesc sisteme fizice mobile de introducere a datelor în reţea (USB Stick, dischetă, CD, etc.)

d) să prevină manifestarea erorilor de proiectare ale aplicaţiilor ce realizează diverse servicii, precum şi punctele slabe ce decurg din exploatarea acestor greşeli.

Firewall-urile se pot clasifica în funcţie de modul de operare în următoarele categorii :

a) firewall filtru de pachete: în funcţie de protocolul de comunicare utilizat, de adresa IP şi de portul-sursă sau destinaţie, se stabilesc reguli care să permita sau să nu permită trecerea unui pachet de date;

b) firewall server proxy: se utilizează următoarele două modele: Circuit Level Gateway (face o filtrare sumară a pachetelor) şi Application Level Gateway (ţine cont de aplicaţiile care schimbă pachete);

c) firewall bazat pe controlul stării conexiunii şi pe istoricul acesteia (dacă o conexiune a fost considerată la un moment dat sigură, se verifică dacă starea actuală a conexiunii este în concordanţă cu cea anterioară).

Un firewall eficient trebuie să includă şi un sistem de detectare a posibilelor atacuri (Intrusion Detection System).

ACTIVITATEA DE ÎNVĂŢARE NR.3

1. Realizaţi un eseu care să trateze implementarea unor nivele de securitate, pe baza următoarelor idei: aplicaţii antivirus(anti-malware) şi firewall, criptarea datelor, politici de backup, coduri de conduită în navigarea pe internet şi politici de management a parolelor. Dimensiunea eseului trebuie să fie de minim o pagină.

2. Realizaţi un rezumat asupra modalităţilor de detecţie ale antiviruşilor. Va trebui să atingă următoarele idei: identificarea bazată pe semnătură, identificarea bazată pe comportament, metoda heuristică, semnături generice.

TEMA 2

Dezvoltarea unei politici de securitate în reţea

TEORIE. FIŞA 4
Prezentarea soluţiilor de protecţie

Importanţa aspectelor de securitate în reţelele de calculatoare a crescut odată cu extinderea prelucrărilor electronice de date şi a transmiterii acestora prin intermediul reţelelor. În cazul operării asupra unor informaţii confidenţiale, este important ca avantajele de partajare şi comunicare aduse de reţelele de calculatoare să fie susţinute de facilităţi de securitate substanţiale. Acest aspect este esenţial în condiţiile în care reţelele de calculatoare au ajuns să fie folosite inclusiv pentru realizarea de operaţiuni bancare, cumpărături sau plata unor taxe.

Persoanele care atentează la securitatea reţelelor pot aparţine unor categorii diverse, comiţând delicte mai mult sau mai puţin grave: sunt cunoscute cazurile de studenţi care se amuză încercând să fure poşta electronică a celorlalţi, **"hacker"-i** care testează securitatea sistemelor sau urmăresc să obţină în mod clandestin anumite informaţii, angajaţi care pretind că au atribuţii mai largi decât în realitate, accesând servicii care în mod normal le-ar fi interzise, sau foşti angajaşi care urmăresc să distrugă informaţii ca o formă de răzbunare, oameni de afaceri care încearcă să descopere strategiile adversarilor, persoane care realizează fraude financiare (furtul numerelor de identificare a cărţilor de credit, transferuri bancare ilegale etc.), spioni militari sau industriali care încearcă să descopere secretele/strategiile adversarilor, sau chiar terorişti care fură secrete strategice.

Problemele de asigurare a securităţii reţelelor pot fi grupate în următoarele domenii interdependente:

- *confidenţialiatea* se referă la asigurarea accesului la informaţie doar pentru utilizatorii autorizaţi şi împiedicarea accesului pentru persoanele neautorizate;
- *integritatea* se referă la asigurarea consistenţei informaţiilor (în cazul transmiterii unui mesaj prin reţea, integritatea se referă la protecţia împotriva unor tentative de falsificare a mesajului);
- *autentificarea* asigură determinarea identităţii persoanei cu care se comunică (aspect foarte important în cazul schimbului de informaţii confidenţiale sau al unor mesaje în care identitatea transmiţătorului este esenţială);
- *ne-repudierea* se referă la asumarea responsabilităţii unor mesaje sau comenzi, la autenticitatea lor. Acest aspect este foarte important în cazul contractelor realizate între firme prin intermediul mesajelor electronice: de exemplu, un contract / comandă cu o valoare foarte mare nu trebuie să poată fi ulterior repudiat(ă) de una din părţi (s-ar putea susţine, în mod fraudulos, că înţelegerea iniţială se referea la o sumă mult mai mică).

Aspectele de securitate enumerate anterior se regăsesc, într-o oarecare măsură, şi în sistemele tradiţionale de comunicaţii: de exemplu, poşta trebuie să asigure integritatea şi confidenţialitatea scrisorilor pe care le transportă. În cele mai multe situaţii, se cere un document original şi nu o fotocopie. Acest lucru este evident în serviciile bancare. În mesajele electronice însă, distincţia dintre un original şi o copie nu este deloc evidentă.

Procedeele de autentificare sunt foarte răspândite şi ele: recunoaşterea feţelor, vocilor a scrisului sau a semnăturilor unor persoane pot fi încadrate în această categorie. Semnăturile şi sigiliile sunt metode de autentificare folosite extrem de frecvent. Falsurile pot fi detectate de către experţi în grafologie prin analiza scrisului şi chiar a hârtiei folosite. Evident, aceste metode nu sunt disponibile electronic şi trebuie găsite alte soluţii valabile.

Dintr-un punct de vedere mai pragmatic, implementarea unor mecanisme de securitate în reţelele de calculatoare de arie largă, în particular – Internet-ul, priveşte rezolvarea următoarelor aspecte:

1. Bombardarea cu mesaje – aşa numitul spam – trimiterea de mesaje nedorite, de obicei cu un conţinut comercial. Programele de e-mail pot încorpora facilităţi de blocare a mesajelor de tip "spam" prin descrierea de către utilizator a unor acţiuni specifice de aplicat asupra mesajelor, în funcţie de anumite cuvinte cheie sau de adresele (listele de adrese) de provenienţă.

2. Rularea unui cod (program) dăunător, adesea de tip virus - acesta poate fi un program Java sau ActiveX, respectiv un script JavaScript, VBScript etc. Cea mai mare parte a programelor de navigare permit utilizarea unor filtre specifice pe baza cărora să se decidă dacă un anumit program va fi rulat sau nu, şi cu ce restricţii de securitate.

3. Infectarea cu viruşi specifici anumitor aplicaţii - se previne prin instalarea unor programe antivirus care detectează viruşii, devirusează fişierele infectate şi pot bloca accesul la fişierele care nu pot fi "dezinfectate". În acest sens, este importantă devirusarea fişierelor transferate de pe reţea sau ataşate mesajelor de e-mail, mai ales dacă conţin cod sursă sau executabil, înainte de a le deschide sau executa.

4. Accesarea prin reţea a calculatorului unui anumit utilizator şi "atacul" asupra acestuia. La nivelul protocoalelor de reţea, protejarea accesului la un calculator sau la o reţea de calculatoare se realizează prin mecanisme de tip firewall, prin comenzi specifice. Acestea pot fi utilizate şi în sens invers, pentru a bloca accesul unui calculator sau a unei reţele de calculatoare la anumite facilităţi din Internet.

5. Interceptarea datelor în tranzit şi eventual modificarea acestora – snooping. Datele se consideră interceptate atunci când altcineva decât destinatarul lor le primeşte. Transmisia protejată a datelor trebuie să garanteze faptul că doar destinatarul primeşte şi citeşte datele trimise şi că acestea nu au fost modificate pe parcurs (datele primite sunt identice cu cele trimise).

6. Expedierea de mesaje cu o identitate falsă, expeditorul impersonând pe altcineva (pretinde că mesajul a fost trimis de la o altă adresă de poştă electronică) – spoofing. Această problemă se rezolvă prin implementarea unor mecanisme de autentificare a expeditorului.

Pentru asigurarea securităţii reţelei este importantă implementarea unor mecanisme specifice pornind de la nivelul fizic (protecţia fizică a liniilor de transmisie), continuând cu proceduri de blocare a accesului la nivelul reţelei (firewall), până la aplicarea unor tehnici de codificare a datelor (criptare), metodă

specifică pentru protecţia comunicării între procesele de tip aplicaţie care rulează pe diverse calculatoare din reţea.

Împiedicarea interceptării fizice este în general costisitoare şi dificilă; ea se poate realiza mai facil pentru anumite tipuri de medii (de exemplu, detectarea interceptărilor pe fibre optice este mai simplă decât pentru cablurile cu fire de cupru). De aceea, se preferă implementarea unor mecanisme de asigurare a securităţii la nivel logic, prin tehnici de codificare/criptare a datelor transmise care urmăresc transformarea mesajelor astfel încât să fie înţelese numai de destinatar; aceste tehnici devin mijlocul principal de protecţie a reţelelor.

Nu trebuie uitată totuşi şi problema numelor de utilizatori şi a parolelor folosite. Autentificarea la un sistem informatic se face în general pe baza unui nume şi a unei parole. Parola este un cuvânt (şir de caractere) secret prin care un utilizator face dovada identităţii sale. Deşi implicaţiile stabilirii unei parole greu de ghicit sunt evidente, mulţi utilizatori acordă o mică importanţă acesteia dând prilej unor terţe persoane, de obicei rău voitoare, să afle aceste parole.

Necesitatea reţinerii unui număr mare de parole pune probleme multor utilizatori, de aceea preferându-se stabilirea unor parole simple, a unei parole unice (folosită la mai multe conturi), notarea lor în locuri uşor accesibile (şi vizibile!) etc.

O parolă complexă este un şir de caractere compus din litere minuscule, majuscule, cifre şi simboluri (@#&%*…). Complexitatea parolei este dată şi de numărul de caractere ce o compun, o parolă din minim opt caractere fiind considerată bună. De reţinut că timpul necesar pentru aflarea unei parole creşte odată cu numărul de caractere din care este compusă.

ACTIVITATEA DE ÎNVĂŢARE NR.4

1. Realizaţi un eseu din care să reiasă necesitatea atingerii următoarelor arii din cadrul securităţii reţelelor: confidenţialitatea, integritatea, autentificarea, ne-repudierea precum şi implementarea unor mecanisme de securitate pentru protejarea împotriva următoarelor efecte: bombardarea cu mesaje (spam-ul şi flood-ul), rularea de cod dăunător(viruşi), filtrarea documentelor ataşate din cadrul căsuţelor de e-mail, expunerea la snoofing şi spoofing. Dimensiunea eseului trebuie să fie de minim o pagină.

2. Având la dispoziţie mai multe soluţii de protecţie la îndemână, un informatician trebuie să prezinte un raport privind ce trebuie să asigure o astfel de soluţie. Care ar fi criteriile de selecţie a unui astfel de sistem şi de ce ?

TEORIE. FIŞA NR.5

Soluţii de securitate hardware şi software

Conceptul de securitate hardware se referă la posibilităţile de a preveni furtul, vandalismul şi pierderea datelor. Se identifică patru mari concepte:

a) securizarea accesului – posibilitatea de a restricţiona şi urmări accesul la reţea (posibilităţile de a îngrădi clădirile şi de a securiza punctele de acces în cadrul unităţii)

b) securizarea infrastructurii – protejarea caburilor, echipamentelor de telecomunicaţii şi dispozitivelor de reţea – gruparea pe cât posibil în locaţii puternic securizate a tuturor echipamentelor de comunicaţie, camere de supravegheat – cu conectare wireless pentru zone greu accesibile – firewall-uri la nivel hardware, posibilitatea de a monitoriza modificarea cablării şi a echipamentelor intermediare de comunicaţie – ex. monitorizarea switch-urilor, routerelor etc.;

c) securizarea accesului la calculatoare – folosind lacăte pentru cabluri – mai ales pentru laptopuri – carcase ce se pot închide, eventual cutii securizate ce conţin unităţile centrale ale desktop-urilor;

d) securizarea datelor – în special pentru prevenirea accesului la sursele de date – ca de ex. Hard disk-urile externe vor trebui ţinute în carcase prevăzute cu lacăte, precum şi dispozitive de siguranţă pentru stick-uri USB. O atenţie foarte mare trebuie oferită soluţiilor de back-up folosite, suporturile acestor date trebuiesc să fie stocate şi transportate în locaţii şi în condiţii foarte sigure(stricte).

Implementarea unei soluţii de securitate foarte puternice este o procedură foarte dificilă ce implică de multe ori costuri foarte mari, cât şi personal calificat şi foarte disciplinat.

Se încearcă să se găsească un compromis între nivelul de securizare dorit şi implicaţiile implementării acestor restricţii. O dezvoltare a ideii de securizare hardware o reprezintă aşa-numitele elemente de monitorizare hardware a reţelelor. Aceste soluţii sunt echipamente special concepute a întreţine reţele întregi de calculatoare şi vin să înlocuiască echipamentele uzuale.

De multe ori aceste echipamente conţin un întreg ansamblu de soluţii – firewall, antivirus, criptări, IDS (Intrusion Detection System), VPN (virtial private network), trafic snaping. Aceste soluţii se bazează pe cipuri ASIC (Application-Specific Integrated Circuit) care sunt circuite integrate personalizate să efectueze o anumită sarcină (se elimină cazurile generale, implementându-se algoritmi speciali, specializaţi şi optimizaţi). Versiuni similare sunt aşa numitele SoC (System on a Cip) care conţin şi alte blocuri funcţionale (procesare pe 32 de biţi, memorie ROM, RAM, EEPROM, Flash). Aceste echipamente totuşi au preţuri foarte mari, prohibitive pentru companiile mici şi mijlocii, ele folosindu-se în special în cadrul marilor companii multi-naţionale.

Menirea unei soluţii de securitate software este de a înlocui şi eventual de a îmbunătăţi soluţia de tip hardware(decizie luată în special din cauza preţului dispozitivelor hardware specializate). Astfel şi soluţiile software se pot organiza într-un mod asemănător cu cel prezentat în fişa 2.2, cu precizările următoare:

a) la nivelul „accesului” se pot folosi sistemele de monitorizare folosindu-se de coduri de acces, camere de supraveghere cu detecţia mişcării

b) la nivel de „infrastructură” firewall-uri software, sisteme de monitorizare ale reţelei în vederea detectării de modificări la nivel de cablări, schimbări de configurare, declanşări de alarme, etc.;

c) la nivel de „date” – posibilităţi de backup automate, păstrate în diferite locaţii, programe de criptare, etc;

d) la nivelul „calculatoarelor” - IDS (Intrusion Detection Systems) – care pot monitoriza modificările din cadrul codului programelor şi sesizează activitatea „neobişnuită” a reţelei, folosirea de aplicaţii de detectare a elementelor de tip malaware (viruşi, spyware, adware, grayware);

Din alt punct de vedere este foarte important de evidenţiat faptul că aceste soluţii de securitate se mai clasifică şi în funcţie de importanţa lor, astfel, deosebim:

a) aplicaţii de tip firewall – pentru filtrarea datelor din cadrul unei reţele;

b) aplicaţii pentru detectarea codurilor dăunătoare: aplicaţii antivirus, aplicaţii anti-spamware, anti-adware, anti-grayware la nivel de reţea;

c) obligativitatea actualizării de patch-uri pentru sistemele de operare şi aplicaţii instalate pentru a minimiza posibilităţile de infectare folosind breşele de securitate nou apărute.

Toate aceste aplicaţii sunt absolut necesare în orice reţea care este conectată la Internet. Pentru orice companie este foarte important ca pe lângă setările de securitate pe calculatoarele utilizatorilor să aibă soluţii de protecţie şi la nivelul reţelei. Întrucât soluţiile de securitate care se pot seta la nivel de desktop (sau laptop) sunt relativ limitate – în special prin prisma puterii de procesare şi de disciplina şi cunoştinţele utilizatorilor – rămâne să se instaleze şi configureze soluţii dedicate de securitate la nivel de reţea, soluţii de care să se folosească toţi utilizatorii din cadrul ei.

Conform unui studiu al companiei Blue Coat[1] care prezintă primele 5 cele mai bune practici de securitate pentru conectarea la internet, se disting direcţiile de urmat în următoarea perioadă (luni, ani) şi anume:

1. Alăturarea la o comunitate de supraveghere (community watch). Din ce în ce mai mulţi utilizatori, se unesc în comunităţi de supraveghere păstrate în aşa numitele „cloud services” – reţele între care există relaţii bine-stabilite, de încredere şi dependenţă, bazându-se pe concepte de procesare în reţea(folosindu-se astfel de puterea de procesare oferită de fiecare calculator din cadrul ei) – pentru a se proteja unii pe alţii. Când o persoană detectează o ameninţare, aceasta este percepută de fiecare utilizator din cadrul norului (cloud) astfel ajungând să se apere fiecare utilizator. Aceste comunităţi sunt un pas foarte important în asigurarea securităţii deoarece conferă avantaje foarte puternice comparativ cu alte soluţii singulare, deoarece are la dispoziţie mai multe resurse şi soluţii defensive.
2. Schimbarea mentalităţii defensive „one against the Web” (singur împotriva Internetului). Soluţiile personale de protejare împotriva atacurilor criminale care vizează furtul de date, de orice natură, devin foarte repede „învechite” întrucât aceste atacuri devin din ce în ce mai complexe şi mai sofisticate tehnologic. Sistemele de protecţie bazate pe semnături actualizate zilnic sunt forme de protecţie depăşite. Nu se compară aceste soluţii cu ceea ce se poate oferi prin soluţiile cu design hibrid folosite de comunităţile de supraveghere, care se bazează pe servicii

[1] Solution Brief: Top Five Security Best Practices for you Web Gateway în 2009, din 06.05.2009, link http://networking.ittoolbox.com/research/top-five-security-best-practices-for-your-web-gateway-în-2009-19108

de protecţie ce se actualizează odată la 5 minute, beneficiind de serviciile defensive a peste 50 de milioane de utilizatori.

3. Schimbarea politicilor bazate pe „producţie” în politici bazate pe „protecţie”. Dacă soluţia existentă la momentul actual este mai veche de 1 an, atunci această soluţie este bazată pe „producţie” – adică la momentul instalării s-a luat în calcul mărirea productivităţii utilizatorilor prin blocarea de site-uri cu conţinut obscen şi neproductiv(ex. jocuri online). Cum s-a ajuns ca peste 90% din conţinutul malaware să vină de la site-uri populare şi „de încredere”, Internetul-ca un tot unitar - a ajuns să fie principalul „furnizor” de acest conţinut. Pentru protejare de atacuri venite din Internet este necesar să se blocheze toate formele de download venite din partea unor site-uri necunoscute sau cu reputaţii ştirbe, blocând astfel o întreagă cale de acces al ameninţărilor de tip malaware în reţeaua locală.

4. Folosirea de servicii Web real-time (în timp real) de evaluare. Conţinutul Web cuprinde o multitudine de metode de filtrare de adrese URL care actualizează zilnic listele URL statice conţinute de fiecare site. Serviciile Web care oferă posibilitatea de a evalua site-urile devin unelte foarte puternice şi necesare pentru a suplimenta valoare de protecţie oferită de soluţiile de filtrare de URL. Dealtfel aceste servicii oferă un real ajutor şi utilizatorilor finali, oferind informaţii în timp real cu privire la conţinutul paginilor vizitate, utilizatorii bucurându-se de navigări relativ sigure folosind politici de securitate acceptabile.

5. Protejarea utilizatorilor ce se conectează de la distanţă. Posibilitatea de a lucra la distanţă a devenit o foarte importantă unealtă de lucru pentru majoritatea utilizatorilor. Adăugarea unui agent de tip client, legat la o comunitate de supraveghere poate proteja mai bine utilizatorii la distanţă. Centralizarea politicilor de management poate oferi protecţia necesară oferită de filtrarea de conţinut şi blocarea de malware de pe site-urile detectate de o întreaga reţea defensivă a unei comunităţi de supraveghere.

Producătorii de hardware au venit cu soluţia simplă de a oferi un nivel de securitate crescut folosind funcţii bazate pe parole (maxim 8 caractere) pentru accesul la resursele unui calculator, această formă de acces fiind o formă des întâlnită, şi la îndemâna oricui. Este aşa-numita „parolare din BIOS”.

Sunt câteva aspecte care conferă acestei forme de securizare anumite avantaje şi dezavantaje:

- este la îndemâna oricui (se regăseşte în orice laptop sau desktop);
- oferă un grad suplimentar de securitate sistemului, reţelei, etc.;
- se poate securiza doar setările BIOS sau şi partea de bootare (prin parolarea doar a BIOS-ului se pot dezactiva de ex. alte surse pentru bootare);
- are un număr de 3 încercări pentru a introduce parola validă (privit dintr-un anumit punct de vedere este un avantaj, dar poate fi şi un dezavantaj);
- nu se pot securiza datele de pe HDD (cu excepţia unor cazuri speciale – ex. seria IBM ThinkPad), acestea fiind accesibile prin montarea în altă unitate;
- odată blocat sistemul (s-a depăşit nr de încercări pentru introducerea parolei) sistemul este blocat şi este necesară intervenţia specializată (posibile soluţii pentru utilizatorul obişnuit: resetarea BIOS-ului

prin acţionarea unui buton, setarea unui jumper sau scoaterea bateriei CMOS);

- pentru anumite tipuri de BIOS sunt deja cunoscute unele parole „backdoor” care pot oferi acces pe sistem, făcând această formă de securizare inutilă;

ACTIVITATEA DE ÎNVĂŢARE NR.5

1. Tratati una din următoarele teme de studiu:

   - securizarea accesului perimetral,
   - securizarea infrastructurii,
   - securizarea accesului la sistemele de calcul,
   - securizarea datelor.

   Aceste teme vor fi tratate atât din punct de vedere al soluţiilor hardware cât şi software. Se va pune accent pe găsirea avantajelor şi dezavantajelor soluţiilor hardware, respectiv software

Pentru rezolvarea sarcinii de lucru consultaţi Fişa de teorie 5 precum şi sursele de pe Internet.

Tema 3

Ameninţări de securitate a reţelelor

TEORIE. FIŞA 6

Surse de atac

Atacurile îşi au originea nu numai din exteriorul reţelei, dar şi din interior de vreme ce parteneri de afaceri sau angajaţi ai companiei se pot conecta în reţea de la distanţă şi tot mai multe aplicaţii se bazează pe tehnologii de tip wireless pentru acces în reţea. Mobilitatea şi accesul la distanţă sunt la fel de necesare în modul nostru de lucru la fel însă şi confidenţialitatea informaţiilor, intimitatea personală şi stabilitatea în reţea ca mediu de lucru utilizat la schimbul de informaţii în timpul activităţii.

Deosebim următoarele categorii de **„atacatori**" sau hackers:

a) pentru distracţie, „for fun", prostie(*script-kid*): sunt cei care fac "prostii" pe net doar ca să se distreze sau să dovedească lor sau altora că sunt posesorii unor skill-uri mai speciale;

b) pentru bani(*well know hackers*), un nivel superior, mult mai profesional de multe ori: sunt cei care fac bani din această "meserie". Aici sunt incluse şi activităţile de spionaj industrial sau corporatist;

c) pentru răzbunare: clienţi nemulţumiţi, foşti angajaţi, competitori sau oameni care au ceva împotriva cuiva dintr-o companie.

Ca surse de atac se disting două mari categorii:

- atacuri din interiorul reţelei;
- atacuri din exteriorul reţelei.

Atacul din interiorul reţelei este forma cea mai devastatoare întrucât utilizatorul are acces la o multitudine de resurse şi deoarece politicile de securitate interne nu sunt atât de bine implementate, sau cel puţin nu sunt definite atât de strict din pricina diversităţii necesare unor utilizatori în a accesa informaţiile răspândite prin cadrul organizaţiei. Mai mult ca regulă generală toţi utilizatori interni intră în categoria utilizatorilor „trusted" – de încredere.

Acesta este şi motivul pentru care, în urma unor informaţii detaliate din cadrul unor rapoarte de securitate s-a observat că riscurile cele mai mari vin de la proprii angajaţi.

Un atac din interior poate fi neintenţionat sau deliberat. În categoria atacurilor neintenţionate întră posibilitatea de a „citi" parola de acces a unei alte persoane, sau divulgarea unor parole, sau prin infectarea calculatorului la care lucrează, expunând întreaga companie la riscul de a se infecta cu un virus. Cea de-a doua formă de atac este de departe cea mai periculoasă, pentru că de multe ori aceste persoane deţin cunoştinţe avansate şi pot eventual să-şi ascundă şi urmele operaţiilor efectuate. Din păcate nu există o formă sigură de protecţie pentru aceste forme de atac, singura care poate oferi informaţii cu privire la astfel de atacuri fiind auditarea accesului – dar

aceasta poate face şi mai mult rău prin prisma stresării suplimentare a utilizatorilor din cadrul organizaţiei.

Pentru a se putea înţelege mai bine atacurile din exterior să facem o comparaţie cu o bancă. Astfel primul pas făcut în direcţia implementării unei defensive eficiente este de a “ridica” un FIREWALL ca o barieră în faţa punctului de intrare în reţea. Este ca şi cum am instala o uşă metalică într-o bancă. Un punct de acces prin care tot tracul este monitorizat pe măsură ce intră sau iese din reţea. Orice intrus cu intenţii suspecte trebuie să fie detectat, aşa că al doilea tip de dispozitive de securitate - camerele de supraveghere – vor fi instalate în spatele porţii metalice, cazul băncii.

Pentru o reţea informatică, al doilea nivel de securitate, furnizat din spatele firewall-ului este făcut prin IDS – Intrusion Detection System sau SDI – Sisteme de Detecţie a Intruziunilor. Aceste sisteme detectează atacurile şi declaşează răspunsuri la aceste atacuri şi mai mult, alertează pe diverse căi administratorul de reţea sau alte persoane abilitate.

Câteodată băncile realizează transfer de bani lichizi şi atunci trebuie să se asigure ca în exterior totul va decurge într-un mod sigur. La fel cum băncile folosesc vehicule blindate pentru protecţia transportului de bani lichizi, reţelele informatice utilizează ca mijloc de transport a datelor în spaţiul public tuneluri securizate de date sau VPN (Virtual Private Network), în româneşte: RVP Reţele Virtuale Private. Deoarece în aceste tuneluri există riscul să se intercepteze informaţiile, iar pachetele de date aflate în tunel să fie compromise în timp ce sunt în tranzit, conţinutul pachetelor de date este obligatoriu să fie criptat!

De cele mai multe ori oamenii vor să aibă acces la facilităţile furnizate de banca din alt oraş sau din altă ţară, aşa că o bancă trebuie să se asigure că oamenii care beneficiază de acces de la distanţă au dreptul de a accesa resursele băncii on-line. În mod similar într-o reţea trebuiesc activate sisteme de autentificare care să verifice identitatea persoanei care trimite şi recepţionează informaţia criptată prin tunelul securizat.

Un plan de securitate puternic este unul conceput pe mai multe layere sau straturi, adică implică mai multe soluţii de securitate. În funcţie de fiecare organizaţie sau companie soluţiile diferă.

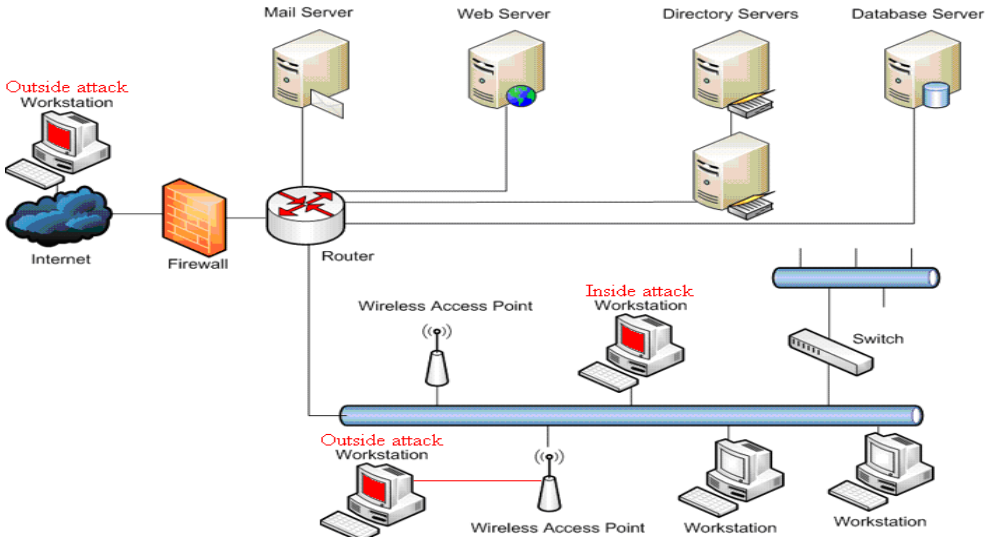


Diagrama privind sursele de atac asupra unei reţele

Cum spuneam mai sus, este necesară instalarea unui firewall care să pună o barieră între cei din afara reţelei, cei din interiorul ei şi modul în care se accesează ea. Astfel, un sistem de tip firewall trebuie să ofere următoarele informaţii:

1. *filtrarea traficului* – sistemul decide ce pachet de date are permisiunea să treacă prin punctul de acces(în concordanţă cu setul de reguli aplicate);

2. *inspectarea fluxurilor de date*, inspectare de tip Statefull (sau filtrarea dinamică a pachetelor) este utilizată pentru a verifica fiecare nou flux de date ce intră în reţea, şi este abilitatea firewall-ului de a memora starea fiecărui flux de date;

3. *NAT* – Network Address Translation – reprezintă o tehnică utilizată pentru a “ascunde” adresele private în spaţiul public.

4. *application gateways* – sunt folosite de aplicaţii precum FTP (File Transfer Protocol) sau RTSP (Real Time Streaming Protocol). Aceste protocoale trimit pachete IP ce conţin adresa fixată a aplicaţiei (socket sau port);

5. *proxy servers* – asigură modul ca o aplicaţie să fie utilizată conform cu politica de securitate specific setată;

6. *detectarea intruziunilor* – pe baza unor şabloane firewall-ul detectează un spectru de atacuri înregistrându-le, notificând administratorul de reţea şi activând un set de acţiuni menit să minimizeze efectul impactului unui atac;

7. *capacităţi de monitorizare şi management al traficului* – evenimentele sunt înregistrate, prelucrate şi prezentate în rapoarte către administratorul de reţea;

8. *mijloace de autentificare* – listele de acces furnizează o cale eficientă de a aplica un mijloc de constrângere unui mare grup de utilizatori aflaţi în spaţiul public.

Un prim pas în aflarea unui mod de penetrare în reţea a unui atacator va fi să afle ce porturi (uşi ascunse) sunt deschise. Pentru aceasta el va face o scanare de porturi. O astfel de metodă totuşi poate fi folosită şi de către administratorul unei reţele pentru a se asigura că este protejat corespunzător.

Scanarea de porturi nu dăunează reţelei sau sistemului, dar asigură hackerului informaţii care pot fi folosite pentru atacuri.

În total avem 65535 porturi TCP (acelaşi număr şi de porturi UDP). Ele sunt folosite de diverse aplicaţii şi servicii. Dacă un port este deschis, el răspunde de fiecare dată când un computer încearcă să-l acceseze prin reţea. Aplicaţiile ce scanează porturi, de tip Nmap, sunt folosite pentru a determina care porturi sunt deschise pe un sistem. Programul trimite pachete pentru o multitudine de protocoale, şi analizând apoi ce răspunsuri primeşte şi ce nu, creează o listă cu porturile ce "ascultă" (listening ports) sau sunt deschise pentru sistemul scanat.

Următoarele porturi sunt cele mai uzuale(cunoscute): 20: FTP(data), 21: FTP(control), 23: Telnet, 25: SMTP, 67: BOOTP server, 68: BOOTP client, 80: http, 88: Kerberos, 110: POP3, 119: NNTP, 194: IRC, 220: IMAPv3, 389: LDAP

Porturile din intervalul 1024-64535 sunt denumite ***registered ports*** ele fiind folosite de către procese şi aplicaţii. Bineînţeles, asta nu înseamnă că aceste porturi nu sunt ţinte ale atacurilor. De exemplu, portul 1433 folosit de SQL poate reprezenta interes pentru hackeri.

O reţea virtuală privată (VPN) este tehnica prin care realizăm "tunele" în spaţiul public, în Internet, pentru a conecta în mod sigur de exemplu birourile unei companii aflate în mai multe locaţii. Pentru VPN-uri bazate pe protocol IP, traficul din reţea este încapsulat în pachetele IP iar acestea sunt transferate prin tunel. Aceasta încapsulare furnizează calea de separare a reţelelor. Autentificarea furnizează verificarea identităţii, iar criptarea furnizează confidenţialitatea datelor încapsulate.

Protocoale utilizate în crearea de tuneluri sunt: MPLS –Multiprotocol Label Switching, GRE – Generic Routing Encapsulation, PPTP – Point-to-Point Tunnelling Protocol, L2TP – Layer 2 Tunnelling Protocol şi nu în ultimul rând IPSec – Internet Protocol Security

Pentru crearea de VPN-uri, pe scară largă este folosit protocolul IPSec. IPSec asigură separarea reţelelor private de cele publice prin tunelarea pachetelor IP în alte pachete IP asigurând totodată confidenţialitatea şi integritatea datelor. IPSec reprezintă o colecţie de alte protocoale înrudite ce operează la Nivelul Reţea(Nivelul 3 în modelul OSI). Deşi IPSec este folosit de cele mai multe ori ca soluţie completă în crearea de VPN-uri, mai poate fi folosit complementar ca schemă de criptare în cadrul VPN-urilor ce au la bază L2TP sau PPTP.

TEORIE. FIŞA 6

Tipuri de atacuri informatice

Când spunem tip de atac ne referim la modul în care un hacker reuşeşte să preia controlul unui sistem şi ce poate el să facă după ce a reuşit penetrarea lui.

Cele mai des întâlnite tipuri de atacuri sunt următoarele:

a) atacuri social engineering;
b) atacuri DoS;
c) scanări şi spoofing;
d) source routing şi alte exploituri de protocoale;
e) exploituri de software;
f) troieni, viruşi şi worms;

Atacurile de tip social engineering. Social engineering aduce în prim plan omul şi greşelile lui. Atacatorul trebuie doar să posede "people skills" sau carismă. Ei câştigă încrederea utilizatorilor (sau şi mai bine, a administratorilor) şi obţin drepturi cu ajutorul cărora se pot conecta pe sisteme. În multe cazuri, această metodă este cea mai uşoară formă de obţinere de acces la un sistem informaţional. Principala metodă de apărare este educarea personalului şi nu implementarea de soluţii tehnice.

Atacuri Denial-of-Service (DoS). Anul 2000, luna februarie. O serie de atacuri DoS au pus la pământ web site-uri că **yahoo.com** sau **buy.com**. Vă daţi seama de forţa acestor atacuri, dacă au putut să doboare astfel de "mamuţi"? Atacurile DoS sunt printre cele mai "populare" printre hackeri atunci când este vizată întreruperea serviciilor unei reţele sau ale unui server. Scopul unui atac DoS este de a genera o cantitate foarte mare de trafic care pune în imposibilitatea de a mai răspunde într-un timp rezonabil a serverelor, routere-lor sau altor echipamente, astfel ele nemaifiind capabile să funcţioneze normal.

Distributed Denial-of-Service. Acest tip de atac face cam acelaşi lucru ca şi DoS-ul, numai că se foloseşte în atingerea scopului său de computere intermediare,

numite agenţi, pe care rulează unele aplicaţii (zombies) care au fost instalate pe calculatoare anterior. Hacker-ul activează de la distanţă aceste "programele" în aşa fel încât toate aceste sisteme intermediare să lanseze atacul DDoS în acelaşi timp. Din cauză că atacul provine de la mai multe calculatoare care pot să fie răspândite prin toată lumea, originea reală a pericolului este foarte greu de găsit. Aşadar DDoS-ul este un pericol dublu. Pe lângă posibilitatea ca reţeaua personală să fie pusă la pământ cu tot cu servere, mai există şi "opţiunea" ca sistemele tale să fie folosite pe post de agenţi intermediari în alte atacuri.

Atacul DNS DoS. Acest tip de atac exploatează diferenţele de mărime între DNS querry (interogarea name server-ului) şi DNS response (răspunsul name server-ului). Atacatorul foloseşte serverele de DNS ca şi amplificatoare pentru a mări traficul de DNS.

Atacul SYN. Atacurile de tip SYN (synchronization request) exploatează *handshake-ul three-way* al protocolului de transport TCP, procesul prin care se stabileşte o sesiune de comunicare între două computere. Deoarece TCP-ul este un protocol de transport connection-oriented, o sesiune sau un link de comunicare unu la unu, one-to-one, trebuie stabilite între cele două sisteme, înainte că ele să poată comunica între ele. Să zicem că un atacator trimite un SYN înspre un server cu un IP sursă spoofed - inexistentă. Normal că server-ul va trimite înspre client un ACK/SYN. Dar cum IP-ul sursă nu este bun, serverul aşteaptă inutil ACK-ul clientului. El nu va veni. Serverul va pune atunci ACK/SYN-ul trimis către client într-o coadă de aşteptare. Această coadă poate stoca un număr limitat de mesaje. Când este plină, toate SYN request-urile care vor urma vor fi ignorate şi serverul va ajunge în postura de a ignora orice cerere venită din partea clienţilor legitimi.

Atacul LAND derivă din cel descris mai sus, cu precizarea că în acest caz, atacatorul în loc să trimită SYN-uri cu adrese IP care nu există, trimite pachete SYN cu adresa IP a clientului-target care este victima în acest caz.

Atacul Ping of Death. Mai este cunoscut şi sub numele de *large packet ping*. Se creează un pachet IP mai mare decât valoarea admisă de specificaţiile protocolului IP, adică 65 536 bytes. Sistemul ţintă este compromis, soluţia fiind un reboot (de multe ori forţat – sistemul blocându-se).

Atacul Teardrop. Acest atac are aceleaşi rezultate ca şi Ping of death, dar metoda este alta. Programul teardrop creează fragmente IP care fac parte dintr-un pachet IP. Problema este că aceste fragmente folosesc *offset fields* (rolul lor este de a indica porţiunea în bytes a acestor fragmente). Problema apare atunci când aceste offset-uri se suprapun. Când computerul ţintă încearcă să reasambleze aceste fragmente în pachetul IP original normal că va genera o problemă (resetare, blocare sau eroare de sistem).

Flood-ul cu ICMP (ping). Se bazează pe o mulţime de pachete ICMP echo request până când se ocupă toată banda disponibilă. Acestui gen de atac i se mai spune şi *ping storm* deoarece luminiţele router-ului sau switch-ului luminează intermitent, cu viteză foarte mare şi interogările în reţea rămân fără răspuns.

Atacul *fraggle* este tot un fel de ping flood. Atacatorul foloseşte un IP clonat (spoofing) şi trimite ping-uri înspre un întreg subnet ca exemplu. Este de menţionat că acest tip de atac a fost folosit în timpul războiului din Kosovo de către hackerii sârbi împotriva siturilor NATO.

Atacul Smurf. Este un fel de agresiune brute force şi foloseşte aceeaşi metodă a flood-ului prin ping, numai că de data asta adresa destinaţie din pachetele ICMP echo request este adresa de broadcast a reţelei. Un router când primeşte astfel de pachete le trimite înspre toate hosturile pe care le "maschează". Pot rezulta cantităţi mari de trafic şi congestionarea reţelei. Combinaţia dintre atacul *fraggle* si cel *Smurf* fac ca reţeaua destinaţie cât şi sursa să fie afectate.

Atacul Mail Bomb. Numele acestui tip de "armă" este edificator. Se trimit aşa de multe mailuri înspre un mail server, încât acesta ajunge în imposibilitatea de a le gestiona, iar userii legitimi nu mai pot beneficia de serviciile acestuia. Din acest tip de atac a derivat unul care presupune "înscrierea" mail serverului la o grămadă de *mailing lists*-liste uneori legitime, care oferă tot felul de informaţii.

Scanning-ul şi spoofing-ul. Termenul de *scanner*, în contextul securităţii în IT, se referă la o aplicaţie software folosită de către hackeri pentru determinarea porturilor TCP sau UDP deschise pe un sistem. Dar şi administratorii este indicat să folosească astfel de aplicaţii, pentru a putea detecta vulnerabilităţile pe sistemele proprii.

Un **virus** este un program creat să distrugă datele sau echipamentele unui calculator. Viruşii sunt programe cu dimensiuni foarte mici, ascunşi fie în fişiere executabile fie ataşaţi unor programe (în acest caz sunt numiţi şi paraziţi). Ei au menirea de a distruge date, să se reproducă (ajungând să blocheze hard discul sau chiar să distrugă motoarele de căutare ale acestuia) şi pot distruge chiar şi componente ale calculatorului.

Sunt două categorii de viruşi informatici:

- ***Hardware*****:** virusi informatici care distrug componente hardware precum hard discul, unităţi optice şi chiar monitorul sau memoria (RAM) unui calculator. Ex. Virusul CIH (1998) care deşi era conţinut în fişiere executabile, avea ca directive să şteargă memoria BIOS şi să o reprogrameze cu linii inutile care făceau calculatorul inutil până la schimbarea cipului.
- ***Software*****:** acei viruşi informatici meniţi să distrugă fişiere sau programe inclusiv sisteme de operare, să modifice structura unui program, să se multiplice până la refuz (umplerea hard discului la maxim (în acest caz blocând motoarele de căutare al acestuia, acestea cedând şi hard discul devine incapabil să mai funcţioneze), să şteargă în totalitate informaţia aflată pe disc, să încetinească viteza de lucru a calculatorului, ajungând, nu de puţine ori in situaţia de a-l bloca.

Câteva detalii de ştiut:

- viruşii se pot înmulţi singuri;
- viruşii sunt creaţi de om;
- un simplu virus se poate multiplica la nesfârşit;
- un virus care se multiplică la nesfârşit este relativ usor de realizat şi chiar şi un virus atât de simplu este periculos pentru că el va ocupa foarte repede memoria disponibilă şi sistemul se va bloca.

Un **worm** este un program sau un algoritm care se multiplică în cadrul unei reţele de calculatoare şi de obicei este periculos pentru că fie folseşte resursele calculatorului innutil, opreşte întreg sistemul sau îl face innoperabil.

Această categorie de viruşi caută să se auto-transmită mai departe ajutându-se de adrese de e-mail, şi poate uneori să ataşeze şi documente furate (parole, informaţii bancare etc.) din calculatorul infestat.

Numim adware sau spyware orice soft care strânge informaţii pe ascuns despre calculatorul utilizatorului prin intermediul conexiunii la Internet a utilizatorului şi fără ştirea lui, de obicei în scopuri publicitare. Aplicaţiile de tip spyware sunt de obicei ascunse în anumite programe gratuite sau de evaluare care pot fi descărcate de pe Internet. Odată instalate programele de tip spyware monitorizează activitatea utilizatorului pe Internet şi transmit aceste informaţii pe ascuns altcuiva.

Programele de tip spyware pot aduna şi transmite informaţii despre adrese de e-mail, parole şi alte date confidenţiale (ID-ul carţii de credit de ex).

Viruşii de tip Cal Tojan

Calul Trojan sunt viruşi care se ascund în spatele altor programe lăsând o uşă din spate (backdoor) deschisă prin care un hacker iţi poate controla calculatorul atunci când eşti conectat la internet. Troienii sunt un fel de viruşi spioni, se instalează fără a atrage atenţia asupra lui, spionează în mod discret şi pregăteşte lovitura finală (aceasta putând fi chiar fatală sistemului). Alte exemplare din categoria troienilor au ca scop principal atacul spre un server, dinspre toate calculatoarele infestate cu acest trojan, trimiţând mii de solicitări pe secundă, făcând serverul să nu mai fie funcţionabil în parametri normali, sau chiar blocându-l.

Spre deosebire de viruşi troienii nu se multiplică singuri, dar pot fi la fel de destructivi ca viruşii.

Unul dintre cele mai întâlnite tipuri de „cal Trojan” este acela care imită un antivirus însă introduce de fapt viruşi în calculatorul tău. Ex. Windows Antivirus 2009 – program care prin denumirea şi aspectul său poate păcăli multă lume să-l instaleze.

ACTIVITATEA DE ÎNVĂŢARE NR. 6

Tratati una din următoarele teme de studiu:

- atacuri social engineering, atacuri DoS,
- atacuri prin troieni, viruşi şi worms,
- atacuri prin exploituri de software sau protocoale.

Se va pune accent pe găsirea unui exemplu pentru fiecare grupă folosind Internetul.

Pentru rezolvarea sarcinii de lucru consultaţi Fişa de documentare 3.2 precum şi sursele de pe Internet.

Tema 4

Securizarea unui sistem de operare

TEORIE.FIŞA 7

Securizare în sisteme Windows XP & Vista

Windows XP este succesorul sistemelor de operare Windows Me şi Windows 2000 şi este primul sistem de operare axat pe consumator produs de Microsoft pe modelul kernel-ului şi a arhitecturii NT. Windows XP a fost lansat pe 25 octombrie 2001 şi a fost vândut în 400 de milioane de exemplare în ianuarie 2006, conform unei estimări făcute de un analist IDC.

Cele mai întâlnite ediţii de Windows XP sunt Windows XP Home Edition, a cărui public ţintă sunt utilizatorii care lucrează la domiciliu şi Windows XP Professional, care are facilităţi adiţionale, ca suportul pentru domeniile Windows Server şi suportul pentru două procesoare fizice, şi este făcut pentru utilizatorii avansaţi şi clienţii de business. Windows XP Media Center Edition este îmbunătăţit cu facilităţi multimedia ce permit utilizatorului să înregistreze şi să vizioneze televiziunea digitală, să vizioneze filme DVD şi să asculte muzică. Windows XP Tablet PC Edition este proiectat să poată rula pe platformele PC-urilor tabletă. Au fost lansate deasemenea Windows XP 64-bit Edition pentru procesoarele IA-64 (Itanium) şi Windows XP Professional x64 Edition pentru x86-64.

Windows XP este cunoscut pentru stabilitatea şi eficienţa sa, în contrast cu versiunile 9x de Microsoft Windows. Prezintă o interfaţă semnificant modificată, mai prietenoasă pentru utilizator decât în celelalte versiuni de Windows. Capacităţile de management noi al software-ului au fost introduse pentru a evita "iadul DLL-urilor" care a marcat celelalte versiuni de Windows. Este prima versiune de Windows care necesită activare pentru a combate pirateria informatică, o facilitate care nu a fost primită cu plăcere de toţi utilizatorii. Windows XP a fost criticat pentru vulnerabilităţile legate de securitate, pentru integrarea aplicaţiilor ca Internet Explorer sau Windows Media Player şi pentru aspecte legate de interfaţa implicită a spaţiului de lucru.

Windows XP Home Edition este proiectat pentru persoane individuale şi include noi experienţe pentru mediile digitale, reţea şi comunicaţii. Include un număr de îmbunătăţiri faţă de Windows 2000 Professional. Astfel:

- software îmbunătăţit şi compatibilitate hardware
- securitate simplificată
- log-are simplificată cu nou ecran “welcome”
- schimbare de utilizator rapidă
- o nouă interfaţă
- suport îmbunătăţit pentru multimedia (filme, poze, muzică)
- DirectX 8.1 pentru jocuri

Windows XP Professional este sistemul de operare destinat oamenilor de afaceri şi firmelor de toate dimensiunile, precum şi tuturor acelor utilizatori individuali care doresc să exploateze la maximum posibilităţile de calcul oferite de PC. La Windows XP Professional se adaugă accesul la distanţă, securitate, performanţă, uşurinţă în utilizare, posibilităţile de conectare.

Cea mai evidentă deosebire însă între Windows XP Home Edition şi Windows XP Professional este securitatea, care este simplificată pentru Windows XP Home Edition. Fiecare utilizator interactiv al Windows XP Home Edition este presupus a fi un membru al grupului local de proprietari (Owners Local Group), care este echivalentul Windows XP al lui Windows 2000 Administrator Account. Aceasta înseamnă că oricine se logează la un calculator cu Home Edition are deplinul control. Totuşi facilităţile Backup Operatores, Power Users şi Replicator Groups deţinute de Windows 2000 sau de Windows XP Professional lipsesc la Windows XP Home Edition. În schimb Windows XP Home Edition beneficiază de un nou grup numit: Restricted Users. Părţile administrative ascunse nu sunt disponibile în Home Edition.

Pentru Windows XP deosebim câteva aspecte foarte importante în vederea asigurării unui nivel de securitate minim:

- discurile să fie formatate în sistem NTFS – prin acest sistem oferindu-se posibilităţi de administrare foarte importante;
- activarea Windows Firewall (sau instalarea unui program de la terţi);
- realizarea de politici clare pentru parole şi obligativitatea introduceri secvenţei CTRL+Alt+Delete pentru logare (anumite programe pot simula această secvenţă pentru realizarea unei conexiuni ascunse);
- Realizarea unor politici la fel de clare privind realizarea de backup–uri la intervale regulate şi nu numai – pentru protejarea datelor în cazuri nedorite;
- Activarea serviciului de Restore Point – procedura ce oferă posibilitatea salvării unor stări de moment ale sistemului;
- Stabilirea unor reguli de acces la Internet Explorer (Zona Local Intranet, pentru site-urile din cadrul organizaţiei sau care se află în spatele firewall-ului utilizatorului, Zona Trusted Sites, pentru site-uri care nu se află în spatele firewall-ului utilizatorului, dar pentru care utilizatorul are încredere totală, Zona Restricted Sites, pentru site-uri cunoscute de utilizator că fiind maliţioase, Zona Internet Zone, pentru restul de site-uri, Zona My Computer, care însă de obicei nu e configurabilă, deoarece controalele ActiveX pe care chiar sistemul de operare le instalează rulează pe setările de securitate din această zonă)

- Nu în ultimul rând este necesară acordarea de atenţie mărită datelor critice cu caracter personal (conturi, parole, documente private) folosindu-se de criptări EFS.

Windows Xp nu vine instalat cu un program antivirus şi de aceea este necesar să se instaleze şi o astfel de aplicaţie (de preferat o soluţie Internet Suite – care conţine şi alte aplicaţii gen anti-spyware, firewall, back-up, etc.).

Windows Vista este cea mai recentă versiune a sistemului de operare Microsoft Windows, proiectată de corporaţia Microsoft. Înainte de anunţul sub acest nume din 22 iulie 2005, Windows Vista a fost cunoscut sub numele de cod **Longhorn**, după Salonul Longhorn, un bar cunoscut din oraşul Whistler din provincia canadiană Columbia Britanică. Windows Vista a fost lansat în noiembrie 2006 pentru firme şi parteneri de afaceri iar în ianuarie 2007 a fost lansat pentru utilizatorii obişnuiţi. Această lansare vine după mai mult de cinci ani de la apariţia pe piaţă a sistemului de operare Windows XP, fiind cea mai mare distanţă între două lansări succesive .

Windows Vista are sute de facilităţi noi, cum ar fi o interfaţă grafică modernă şi un stil vizual nou, Windows Aero, tehnologia de căutare îmbunătăţită, noi unelte multimedia, precum şi sub-sistemele complet remodelate de reţea, audio, imprimare şi afişare (display). Vista va îmbunătăţi comunicarea dintre maşini pe o reţea casnică folosind tehnologia peer-to-peer, şi va facilita folosirea în comun a fişierelor, parolelor, şi mediilor digitale între diverse computere şi dispozitive. Pentru proiectanţii de software, Vista pune de asemenea la dispoziţie versiunea 3.0 a sistemului de proiectare numit .NET Framework.

De o securitate îmbunătăţită putem beneficia folosind şi ultima versiune a aplicaţiei "Windows Firewall" inclusă în sistemul de operare Windows Vista. Dar securitate înseamnă mult mai mult decât updatarea sistemului de operare, o aplicaţie antispyware/antivirus sau o aplicaţie firewall. Un sistem de operare trebuie să ofere încredere utilizatorilor şi să protejeze datele (mai mult sau mai puţin confidenţiale) stocate pe aceste sisteme. În acest domeniu al securităţii (protecţia datelor, identitate şi control acces) intră şi tehnologiile "User Account Control" sau "Internet Explorer 7 – Protected Mode".

"User Account Control" - tehnologie care nu există în Windows XP, apărând prima dată în Windows Vista şi în Windows Server 2008 - reduce posibilitatea că o aplicaţie cu privilegii minime (low) să dobândească în mod **automat** şi **necontrolat** privilegii sporite şi să aibă acces la fişierele utilizatorului fără consimţământul acestuia.

Această posibilitate există în Windows 2000/XP unde un utilizator (cu drepturi de administrator) putea fi indus în eroare mai uşor să execute un anumit cod (aplicaţie ostilă acelui sistem) şi care putea duce la compromiterea acestuia.

În Windows Vista orice aplicaţie care solicită acces la zone sensibile ale sistemului de operare (fişiere de sistem, registry-ul de sistem) va primi acces să ruleze numai după consimţământul explicit al utilizatorului.

Windows Vista introduce conceptul de etichetă (label) şi 4 nivele de integritate: low, medium , high şi system. În mod uzual toţi utilizatorii sistemului de

operare Windows Vista (inclusiv administratorul) rulează la un nivel de integritate "Medium".

În momentul când un utilizator (administrator) trebuie să-şi eleveze (sporească) privilegiile pentru a rula o aplicaţie ce accesează zone sensibile ale sistemului de operare (sistem de fişiere, registry) nivelul sau de integritate devine "High".

Internet Explorer rulează în mod normal la un nivel "Low" de integritate. Orice aplicaţie care se descarcă din Internet va dobândi un nivel de integritate "Low" (egal cu al procesului Internet Explorer) şi nu va putea să se execute şi să-şi eleveze privilegiile compromiţând sistemul respectiv. Acesta este modul protejat (Protected mode) în care rulează IE7 pe Windows Vista. Modul protejat oferit de IE7 este o facilitate prezentă numai pe sistemul de operare Windows Vista.

Atenţie! "User Account Control şi Internet Explorer Protected Mode" se pot dezactiva, dar nu este recomandat. În plus, pentru site-urile web din zona Trusted Sites din Internet Explorer 7 – modul protejat (Protected mode) este dezactivat.

Un utilizator poate accesa şi modifica un obiect în Windows Vista numai dacă nivelul sau de integritate este mai mare decât cel al obiectului.

În acest scop în Windows Vista sunt definite 3 politici obligatorii de acces:

- No WRITE UP – o entitate nu poate modifica un obiect dacă posedă un nivel de integritate mai mic decât al obiectului respective
- No READ UP – o entitate nu poate citi un obiect dacă poseda un nivel de integritate mai mic decât al obiectului respective
- No EXECUTE UP – o entitate nu poate executa un obiect dacă posedă un nivel de integritate mai mic decât al obiectului respectiv

Principii de securitate

Putem privi aceste tehnologii şi prin prisma altui principiu de securitate – "principle of least privilege" sau "principle of minimal privilege" - "principiul privilegiului minim" în care utilizatorul trebuie să aibe privilegii minime pentru accesarea unui sistem informatic conform fişei postului şi sarcinilor pe care trebuie să le îndeplinească.

În acest fel, în Windows Vista toţi utilizatorii au acelaşi nivel de integritate (încredere) pe un sistem iar privilegiile administrative se folosesc doar în cazul în care este necesar.

Aceste tehnologii de securitate sunt o implementare a modelelor de securitate dezvoltate încă din anii ’70 – modelul de integritate a datelor Biba şi modelul de confidenţialitate a datelor Bell – LaPadula.
Mai multe informaţii se găsesc la adresa
http://msdn2.microsoft.com/en-us/library/bb625964.aspx
http://msdn2.microsoft.com/en-us/library/bb625959.aspx .

ACTIVITATEA DE ÎNVĂŢARE NR. 7

Trataţi una din următoarele teme de studiu:

- elemente de securitate în Windows XP Home şi Professional
- elemente de securitate în Windows Vista.

Pentru rezolvarea sarcinii de lucru consultaţi Fişa de mai sus precum şi sursele de pe Internet.

TEORIE.FIŞA 8

Securizarea sistemelor de operare de tip server

Windows Server 2003 este construit pe structura sistemului Windows 2000 şi include toate facilităţile pe care un client le aşteaptă de la un sistem de operare *Windows Server*: siguranţă, securitate şi scalabilitate. Familia cuprinde patru produse:

- *Windows Web Server 2003* reprezintă o bună platformă pentru dezvoltarea rapidă a aplicaţiilor şi desfăşurarea serviciilor pe Web. Este uşor de administrat şi se poate gestiona, de la o staţie de lucru aflată la distanţă, cu o interfaţă de tip browser.
- *Windows Standard Server 2003* este un sistem de operare în reţea care oferă soluţii pentru firmele de toate mărimile. Acceptă partajarea fişierelor şi imprimantelor, oferă conectivitate sigură la Internet, permite desfăşurarea centralizată a aplicaţiilor din spaţiul de lucru, oferă colaborare între angajaţi, parteneri şi clienţi, acceptă multiprocesarea simetrică cu două căi şi până la 4 GO de memorie.
- *Windows Enterprise Server 2003* este destinat firmelor medii şi mari. Este un sistem de operare cu funcţionare completă care acceptă până la 8 procesoare de tip Intel Itanium.
- *Windows Data Center Server 2003* este o platformă pentru firmele cu un volum mare de tranzacţii şi cu baze de date scalabile. Este cel mai puternic şi mai funcţional sistem de operare pentru servere oferit de Microsoft.

În general, sistemele Windows se compun din trei clase de programe: programele sistemului de bază; programele API (Application Programming Interface) şi programele „maşini virtuale”.

Programele sistemului de bază asigură controlul fişierelor, servicii de comunicare şi control în reţea, controlul maşinii virtuale, controlul memoriei, controlul implementării standardului de interconectare „plag&play”.

Sistemul API cuprinde trei componente: nucleul Windows – Kernel, interfaţa grafică cu echipamentele periferice GDI (Graphic Devices Interface) şi componenta

USER. Aceste componente sunt biblioteci de programe adresate programatorului de aplicaţii şi mai puţin utilizatorului obişnuit.

Sistemul „maşini virtuale” asigură interfaţa cu utilizatorul şi aplicaţiile sale, modulele din această clasă fiind apelate de sistemul API. Această componentă asigură încărcarea şi folosirea corectă a spaţiului de adresare. Din această clasă face parte şi programul Explorer.

Atunci când se ia în calcul politica de securitate pentru platformele Windows Server 2003 şi 2008 trebuie evaluate obligatoriu următoarele:

- Domain Level Acount Polices – reguli ce se pot seta la nivel de Group Policies, setări care sunt aplicate la întreg domeniul: politici cu privire la parole, blocarea conturilor, autentificarea folosind protocolul Kerberos – tot ceea ce uzual se înţelege prin „acount polices” – politici de cont;

- Audit Policy – posibilităţile de utilizare a politicilor de audit pentru a monitoriza şi forţa setările de securitate instalate. Este obligatoriu să se explice diferitele setări, folosindu-se de exemple, pentru a se înţelege ce informaţii se modifică când acele setări sunt modificate;

- User Rights – tratează diferitele posibilităţi de logon – drepturi şi privilegii ce sunt puse la dispoziţie de sistemul de operare şi oferirea de îndrumare privind care conturi ar trebui să primească drepturi distincte – şi natura acestor drepturi;

- Security Options – tratarea setărilor de securitate cu privire la date criptate cu semnături digitale(digital data signature), statutul conturilor „Administrator” şi „Guest”, accesul la unităţile de dischetă şi CD-ROM(sau echivalent), instalarea driver-elor şi posibilităţile de logare(logon prompts);

- Event Log – configurarea setărilor pentru diferitele jurnale care există sum Windows Server 2003(respectiv 2008);

- System services – utilizarea serviciilor care sunt absolut necesare şi documentarea lor – dezactivarea serviciilor care nu sunt folosite sau necesare. Personalizarea pe cât posibil a acestor servicii – pentru eliminarea setărilor „by default”;

- Software restriction polices – descrierea pe scurt a software-ului instalat şi mecanismele folosite pentru restricţia rulării acestora;

- Additional System Countermeasures – descrierea unor măsuri suplimentare de securitate care sunt necesare, setări care rezultă din discuţia privind rolul acelui server, posibilităţile de implementare, disponibilitatea utilizatorilor şi existenţă personalului calificat – setări cum ar fi:setări care nu pot fi introduse îîntr-o maniera compactă în cadrul Group Policies, setări la nivel de drepturi pe fisiere (NTFS), SNMP, dezactivarea NetBIOS, setări Terminal Services, setări IPsec, Dr. Watson, nu în ultimul rând setările cu privire la Windows Firewall.

- Additional Registry Entries – documentarea modificărilor necesare la nivel de registri;

Este de reţinut faptul că în Windows 2008 s-a pus un accent mai mare pe securitate , ca un exemplu dacă în Windows 2003 server cu SP1 erau în jur de 1700 de setări în Group Polices în Windows 2008 Server a crescut la aproximativ 2400.

Fiecare elev(ă) sau grupă va trebui să completeze în tabelul următor, în coloana „Denumire” cu elementele corespondente din lista: Security Options, Domain Level Acount Polices, Event Log, Audit Policy, User Rights, System services, Software restriction polices, Additional Registry Entries, Additional System Countermeasures.

Denumire	Descriere
	Un set de reguli ce se pot seta la nivel de Group Policies, setări care sunt aplicate la întreg domeniul: politici cu privire la parole, blocarea conturilor, autentificarea folosind protocolul Kerberos, etc.
	Reprezintă posibilităţile de utilizare a politicilor de auditare pentru a monitoriza şi forţa setările de securitate instalate.
	Tratează diferitele posibilităţi de logare precum şi drepturi şi privilegii ce sunt puse la dispoziţie de sistemul de operare şi oferirea de îndrumare privind conturi care ar trebui să primească drepturi distincte (evidenţierea acestor drepturi)
	Tratarea setărilor de securitate cu privire la date criptate cu semnături digitale (digital data signature), statutul conturilor „Administrator” şi „Guest”, accesul la unităţile de dischetă şi CD-ROM (sau echivalent), instalarea driver-elor şi posibilităţile de logare (logon prompts);
	Utilizarea serviciilor care sunt absolut necesare şi documentarea lor – dezactivarea serviciilor care nu sunt folosite sau necesare.
	Configurarea setărilor pentru diferitele jurnale care există sum Windows Server 2003 (respectiv 2008);
	Descrierea unor măsuri suplimentare de securitate care sunt necesare, setări care rezultă din discuţia privind rolul acelui server, posibilităţile de implementare, disponibilitatea utilizatorilor şi existenţa personalului calificat.
	Descrierea pe scurt a software-ului instalat şi mecanismele folosite pentru restricţia rulării acestora
	Documentarea modificărilor necesare la nivel de registri;

Pentru rezolvarea sarcinii de lucru consultaţi Fişa de documentare 4.2 precum şi sursele de pe Internet.

ACTIVITATEA DE ÎNVĂŢARE NR. 8

1. Fiecare elev(ă) va trebui să completeze în tabelul următor, în coloana „Denumire” cu elementele corespondente din lista: Security Options, Domain Level Acount Polices, Event Log, Audit Policy, User Rights, System services, Software restriction polices, Additional Registry Entries, Additional System Countermeasures.

Denumire	Descriere
	Un set de reguli ce se pot seta la nivel de Group Policies, setări care sunt aplicate la întreg domeniul: politici cu privire la parole, blocarea conturilor, autentificarea folosind protocolul Kerberos, etc.
	Reprezintă posibilităţile de utilizare a politicilor de auditare pentru a monitoriza şi forţa setările de securitate instalate.
	Tratează diferitele posibilităţi de logare precum şi drepturi şi privilegii ce sunt puse la dispoziţie de sistemul de operare şi oferirea de îndrumare privind conturi care ar trebui să primească drepturi distincte (evidenţierea acestor drepturi)
	Tratarea setărilor de securitate cu privire la date criptate cu semnături digitale (digital data signature), statutul conturilor „Administrator” şi „Guest”, accesul la unităţile de dischetă şi CD-ROM (sau echivalent), instalarea driver-elor şi posibilităţile de logare (logon prompts);
	Utilizarea serviciilor care sunt absolut necesare şi documentarea lor – dezactivarea serviciilor care nu sunt folosite sau necesare.
	Configurarea setărilor pentru diferitele jurnale care există sum Windows Server 2003 (respectiv 2008);
	Descrierea unor măsuri suplimentare de securitate care sunt necesare, setări care rezultă din discuţia privind rolul acelui server, posibilităţile de implementare, disponibilitatea utilizatorilor şi existenţa personalului calificat.
	Descrierea pe scurt a software-ului instalat şi mecanismele folosite pentru restricţia rulării acestora
	Documentarea modificărilor necesare la nivel de registri;

Pentru rezolvarea sarcinii de lucru consultaţi Fişa de documentare 4.2 precum şi sursele de pe Internet.

Tema 5

Configurarea serviciilor de audit şi jurnalizare la sistemele de operare

TEORIE.FIŞA 9

Configurarea serviciilor de jurnalizare şi audit

Auditul sistemelor informatice se defineşte ca examinarea unui sistem informatic şi comparare lui cu prevederile unui standard agreat.

Auditul sistemelor informatice reprezintă activitatea de colectare şi evaluare a unor probe pentru a determina dacă sistemul informatic este securizat, menţine integritatea datelor prelucrate şi stocate, permite atingerea obiectivelor strategice ale întreprinderii şi utilizează eficient resursele informaţionale. În cadrul unei misiuni de audit a sistemului informatic cele mai frecvente operaţii sunt verificările, evaluările şi testările mijloacelor informaţionale.

Principalele tipuri de audit informatic sunt:

- auditul sistemului operaţional de calcul presupune revizia controalelor sistemelor operaţionale de calcul şi a reţelelor, la diferite niveluri; de exemplu, reţea, sistem de operare, software de aplicaţie, baze de date, controale logice/procedurale, controale preventive /detective /corective etc;
- auditul instalaţiilor IT include aspecte cum sunt securitatea fizică, controalele mediului de lucru, sistemele de management şi echipamentele IT;
- auditul sistemelor aflate în dezvoltare acoperă unul sau ambele aspecte: (1) controalele managementului proiectului şi (2) specificaţiile, dezvoltarea, testarea, implementarea şi operarea controalelor tehnice şi procedurale, incluzând controalele securităţii tehnice şi controalele referitoare la procesul afacerii;
- auditul managementului IT include: revizia organizaţiei, structurii, strategiei, planificării muncii, planificării resurselor, stabilirii bugetului, controlul costurilor etc.; în unele cazuri, aceste aspecte pot fi auditate de către auditorii financiari şi operaţionali, lăsând auditorilor informaticieni mai mult aspectele tehnologice;
- auditul procesului IT – revederea proceselor care au loc în cadrul IT cum sunt dezvoltarea aplicaţiei, testarea, implementarea, operaţiile, mentenanţa, gestionarea incidentelor;
- auditul managementului schimbărilor prevede revizia planificării şi controlului schimbărilor la sisteme, reţele, aplicaţii, procese, facilităţi etc., incluzând managementul configuraţiei, controlul codului de la dezvoltare, prin testare, la producţie şi managementul schimbărilor produse în organizaţie;
- auditul controlului şi securităţii informaţiilor implică revizia controalelor referitoare la confidenţialitatea, integritatea şi disponibilitatea sistemelor şi datelor;
- auditul conformităţii cu legalitatea se referă la copyright, conformitate cu legislaţia, protecţia datelor personale;

Pentru realizarea un set de politici şi proceduri pentru managementul tuturor proceselor IT într-o organizaţie s-a definit un set îndrumător sub numele de CoBIT. Acest model (în varianta 4.1) ilustrativ se poate modela că o împărţire a IT-ului în 4 domenii şi 34 de procese în line cu responsabilitatea ariilor de acoperire, construire şi monitorizare oferind o soluţie de la cap la coadă pentru întreg conceptul IT.

Rezumat la conceptul de arhitectură la nivel de întreprindere, ajută foarte mult să se identifice resursele esenţiale pentru succesul proceselor, de ex. – aplicaţii, informaţii, infrastructură şi oameni.

Un alt sistem de auditare este oferit spre certificare folosindu-se standardul ISO/IEC 17799:2000 – set de politici care odată implementat este sinonim cu atingerea unui nivel ridicat de securitate IT(acest standard este agreat şi de Comisia Europeană).

Deşi acest standard conferă băncilor care doresc să implementeze un system de internet banking, autorizaţia de funcţionare – autorizaţie care se va face în fiecare an, de către o companie independentă cu competenţe solide în activităţi de securitate informatică, el poate fi folosit ca şi ghid pentru celelalte domenii.

În mod uzual în ţara noastră se folosesc 3 categorii de auditare:

Auditul specializat – 1 – care asigură conformităţile cu prevederile Ordinului MCTI nr. 16/24.01.2003 este adresat furnizorilor de servicii care doresc eliminarea birocraţiei prin listarea unui singur exemplar de factură fiscală. Este auditat planul de securitate al sistemului informatic, iar analiza este efectuată anual de către o echipă independentă, specializată, care are în componenţă şi membri certificaţi CISA.

Auditul specializat 2 – se referă la auditarea planului de securitate în vederea aplicării prevederilor Ordinului Min. Finanţelor nr. 1077/06.08.2003 şi presupune scanarea de vulnerabilităţi – adică este testată vulnerabilitatea unui sistem informatic la atacuri din afară sau din interiorul reţelei. Este analizat modul în care sunt configurate echipamentele de reţea, sistemele de operare de pe staţii şi servere şi se compară cu recomandările de securitate ale producătorului. Acest tip de audit de securitate este executat de către un specialist certificat şi experimentat pe produsul auditat.

Auditul specializat 3 – se referă la securitatea infrastructurii IT. Această formă de audit de securitate presupune know-how, experienţă, specialişti şi certificări.

Relativ la sistemele de operare şi jurnalizarea informaţiilor din sistem, se deosebesc trei tipuri de jurnale: jurnalul de aplicaţii, jurnalul de securitate şi jurnalul de sistem.

Tipuri de jurnal de evenimente

- Jurnalul de aplicaţii (Application log). Jurnalul de aplicaţii conţine evenimentele înregistrate de programe. De exemplu, un program de baze de date poate înregistra o eroare de fişier în jurnalul de aplicaţii. Evenimentele ce se scriu în jurnalul de aplicaţii sunt determinate de dezvoltatorii programului software.
- Jurnalul de securitate (Security log). Jurnalul de securitate înregistrează evenimente precum încercările valide şi invalide de Log on, precum şi evenimentele legate de utilizarea resurselor, cum ar fi crearea, deschiderea sau ştergerea de fişiere. De exemplu, când este activată auditarea la Log on, este înregistrat un eveniment în jurnalul de securitate de fiecare dată când un utilizator face Log on pe computer. Trebuie să faceţi Log on ca administrator sau ca membru al grupului de administratori pentru a activa, utiliza şi specifica evenimentele de înregistrat în jurnalul de securitate.
- Jurnalul de sistem (System log). Jurnalul de sistem conţine evenimente înregistrate de componentele de sistem. De exemplu, dacă un driver nu reuşeşte să se încarce în timpul pornirii, va fi înregistrat un eveniment în jurnalul de sistem.

Sistemele bazate pe platforma Windows determină anticipat evenimentele înregistrate de componentele de sistem.

Modul de interpretare a unui eveniment

Fiecare intrare din jurnal este clasificată prin tipul său şi conţine informaţii de antet şi o descriere a evenimentului.

Antetul evenimentului

Antetul evenimentului conţine următoarele informaţii despre eveniment:

- Date: Data la care s-a produs evenimentul.
- Time: Ora la care s-a produs evenimentul.
- User: Numele de utilizator al utilizatorului care era conectat când s-a produs evenimentul.
- Computer: Numele computerului pe care s-a produs evenimentul.
- Event ID: Un număr care identifică tipul evenimentului. ID-ul evenimentului poate fi utilizat de reprezentanţii serviciului de asistenţă pentru produs pentru a înţelege ce anume s-a întâmplat în sistem.
- Source: Sursa evenimentului. Aceasta poate fi numele unui program, o componentă de sistem sau o componentă individuală a unui program mare.
- Type: Tipul evenimentului. Există cinci tipuri de evenimente: Error, Warning, Information, Success Audit sau Failure Audit.
- Category: O clasificare a evenimentului în funcţie de sursa evenimentului. Aceasta este utilizată în principal în jurnalul de securitate.

Tipuri de evenimente. Descrierea fiecărui eveniment înregistrat depinde de tipul evenimentului. Fiecare eveniment dintr-un jurnal poate fi clasificat într-unul din următoarele tipuri:

- Information: Un eveniment care descrie desfăşurarea cu succes a unei activităţi, cum ar fi o aplicaţie, un driver sau un serviciu. De exemplu, un eveniment de informare este înregistrat când se încarcă cu succes un driver de reţea.

- Warning: Un eveniment care nu este neapărat important poate totuşi să indice apariţia unei probleme în viitor. De exemplu, un mesaj de avertizare este înregistrat când spaţiul liber pe disc începe să fie scăzut.

- Error: Un eveniment care descrie o problemă importantă, precum eroarea unei activităţi critice. Evenimentele de eroare pot implica pierderi de date sau de funcţionalitate. De exemplu, un eveniment de tip eroare este înregistrat dacă un serviciu nu reuşeşte să se încarce în timpul pornirii.

- Success Audit (în jurnalul de securitate): Un eveniment care descrie completarea cu succes a unui eveniment de securitate auditat. De exemplu, un eveniment de tip auditare reuşită este înregistrat când un utilizator face Log on pe computer.

- Failure Audit (în jurnalul de securitate): Un eveniment care descrie un eveniment de securitate auditat care nu s-a terminat cu succes. De exemplu, un eveniment de tip auditare nereuşită se înregistrează când un utilizator nu poate accesa o unitate de reţea.

Gestionarea conţinutului jurnalului

În mod implicit, dimensiunea iniţială maximă a jurnalului este setată la 512 KO şi când se ajunge la această dimensiune evenimentele noi se suprascriu peste cele vechi. În funcţie de nevoile dvs., aveţi posibilitatea să modificaţi aceste setări sau să goliţi un jurnal de conţinutul său.

Dacă doriţi salvarea datelor jurnalului, aveţi posibilitatea să arhivaţi jurnalele de evenimente în oricare dintre următoarele formate:

- Format fişier jurnal (.evt)
- Format fişier text (.txt)
- Format fişier text cu delimitator virgulă (.csv)

Pentru o mai bună gestionare a acestor fisiere – raportări diferite, căutări încrucişate, etc. se pot folosi diferite programe care “traduc” aceste fisiere în forme vizuale cu detalierea informaţiilor prezentate. Soluţiile profesionale – de obicei folosite pe servere sunt aşa numitele **Log Processing System (LPS) care** oferă suport pentru procesarea în timp real a logurilor generate de diverse servere din reţeaua dumneavoastră şi raportarea imediată a evenimentelor detectate.

- Permite cunoasterea imediata şi permanentă a stării reţelei, în detaliu. Procesarea logurilor funcţionează pe baza de plug-in-uri configurabile în funcţie de necesităţile de monitorizare a clientului
- Permite analiza oricărui fişier de log, a oricărei aplicaţii, pentru monitorizarea activităţii afacerii şi din alte puncte de vedere decât securitatea tehnologică a informaţiei
- Facilitează separarea alarmelor false de cele reale, reducând cantitatea de munca a personalului tehnic
- Accelereaza procesele de reacţie în caz de atac, prin indicarea clară a zonelor şi staţiilor vulnerabile

Plugin-uri LPS diponibile:

- WSPT - Windows Station Process Tracking - raportează data şi durata execuţiei aplicaţiilor instalate;
- WSSA - Windows Server Share Access - raportează accesul pe un director partajat identificând serverul, utilizatorul, domeniul şi activităţile întreprinse - scriere, citire, modificare;
- GWEL - Generic Windows Event Log - asigură procesarea generică de log-uri Windows privind aplicaţiile rulate şi evenimentele de securitate;
- ASLP - Axigen Server Log Processor - asigură procesarea informaţiilor privind schimburile de corespondenţă;
- WPLA - Web Proxy Log Analyzer - oferă informaţii privind adresele web accesate de utilizatori, durata şi traficul efectuat;

SPMM - Server Performance Monitoring Module - asigură procesarea datelor specifice funcţionării serverelor - nivelul de solicitare al procesorului, memoria utilizată, spaţiul disponibil pe HDD;

ACTIVITATEA DE ÎNVĂŢARE NR. 9

1. Fiecare elev(ă) va trebui să completeze spaţiile punctate cu elementele precizate mai jos.

- Există trei mari categorii de jurnale: de ……., de ……. şi de ……. Jurnalul de ……. conţine evenimentele înregistrate de programe. De exemplu, un program poate înregistra o eroare de fişier în acest jurnal. Evenimentele ce se scriu în jurnalul de ……. sunt determinate de producătorii programului software. Jurnalul de ……. înregistrează evenimente precum încercările valide şi invalide de Log on, precum şi evenimentele legate de utilizarea resurselor, cum ar fi crearea, deschiderea sau ştergerea de fişiere. De exemplu, când este activată auditarea la Log on, este înregistrat un eveniment în jurnalul de ……. de fiecare dată când un utilizator face Log on pe computer. Trebuie să fiţi conectat ca administrator sau ca membru al grupului de administratori pentru a activa, utiliza şi specifica evenimentele de înregistrat în jurnalul de ……. Jurnalul de ……. conţine evenimente înregistrate de componentele de sistem. De exemplu, dacă un driver nu reuşeşte să se încarce în timpul pornirii, va fi înregistrat un eveniment în jurnalul de ……. Sistemele bazate pe platforma Windows determină anticipat evenimentele înregistrate de componentele de sistem.

Se vor completa spaţiile punctate cu unul dintre cuvintele: sistem, aplicaţii sau securitate.

Pentru rezolvarea sarcinii de lucru consultaţi Fişa de documentare 5.1 precum şi sursele de pe Internet.

FISA 10

Routerul – serverul modern

ROUTERUL – este un dispozitiv care conecteaza doua sau mai multe calculatoare alaturi de alte dispozitive (tablete, telefoane inteligente, DVR-ul (digital video recorder), console de jocuri). Acestea toate la un loc poarta numele de clienti.

Configurarea ROUTERULUI

a. Se conectează routerul la sursa de alimentare
b. Se conectază conectorul WAN (conectorul RJ-45 de la furnizorul de internet)
c. Se conecteaza prin cablu UTP (gasit în cutia routerului)la unul din conectorii LAN calculatorul
d. Se porneste routerul si calculatorul astfel conectati

Primul pas este configurarea calculatorului (calculatoarelor) ce sunt legate la router. Acestea trebuie sa fie configurate astfel incat sa obtina adresa de IP in mod automat.

Majoritatea routerelor au adresa de IP de forma : **192.168.0.1** sau **192.168.1.1**. Aceasta adresa IP este data de softul routerului care acum joaca rolul unui server. De obicei Aceasta se poate afla din manualul routerului, iar in caz că nu avem acces la manual deschidem fereastra comand prompt si tastăm comanda ***ipconfig.***

Adresa routerului este adresa " Default Gateway" el fiind acum după cum spuneam mai sus serverul care o sa vedem in continuare aloca adrese de IP dispozitivelor legate la router.

Configurarea propriu – zisă :

1. Deschideţi un browser web şi tastaţi adresa IP a routerului (implicit este 192.168.1.1) în câmpul adresă şi apoi apăsaţi **Enter**.
2. Introduceţi numele de utilizator şi parola pe pagina de autentificare, ambele sunt în mod implicit **admin** (le gasiți în manualul de utilizare sau pe partea inferioară a routerului) .
3. Mergem în partea stângă a ecranului și facem clic pe „**quick setup**”.
4. Apoi aici apăsăm pe NEXT
5. Urmează sa alegem una din obțiuni în funcție de caracteristicile conexiuni de internet furnizate de provaider (firma furnizoare a conexiunii la internet).
6. In cazul în care nu știți tipul conexiunii dați click pe obțiunea : **Auto-Detect** și veți fi direcționat spre completarea datelor în funcție de conexiune. În continuare vom particulariza pentru tipul de conexiune **PPPoE**
7. Scriem numele de utilizator și parola pe care le-am primit de la furnizorul de internet. Odată numele și de două ori parola.
8. Urmează configurarea rețelei wireless unde trebuie sa introduceți numele rețelei (SSID) și parola pentru conectare wireless pentru a elimina conexiunile nedorite (neautorizate)
9. Urmează ultimul pas în care suntem “felicitaţi” pentru succesul configurării , iar dupa repornirea routerului (reboot) putem să ne conectăm la internet atât cu dispozitivele legate prin cablu UTP (PC-uri) cât şi cu dispozitive wireless introducând binenţeles parola configurată în router. Fiecarui dispozitiv conectat la router acestuia i aloca o adresa IP el jucand rolul unui server de aici si denumirea de server modern!

Activitatea de invatare 10

1. Faceţi un referat de maxim o pagină cu titlul „ ROUTER vs SERVER în care să descrieţi principalele asemănări şi deosebiri ale fiecărui dispoztiv de reţea
2. În prezentarea de mai sus securitatea wireless s-a făcut prin parolă. Descrieţi cum se poate face acest lucru prin adresa mac a dispozitivelor din reţea.
3. Cu ajutorul unui router (ca cel prezentat mai sus) cum se poate face securizarea reţelei prin accesul condiţionat de IP
4. Ce reprezintă „ Controlul parental “ aflat în panoul stâng al routerului.